

# What protection do children in Jersey have from online harms?

Children, Education and Home Affairs Scrutiny Panel

7<sup>th</sup> November 2025

S.R. 4/2025



States of Jersey  
States Assembly



États de Jersey  
Assemblée des États



|                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------|----|
| Chair’s Foreword.....                                                                                 | 5  |
| Executive Summary .....                                                                               | 6  |
| Findings and Recommendations .....                                                                    | 11 |
| Key Findings.....                                                                                     | 11 |
| Key Recommendations .....                                                                             | 12 |
| Findings.....                                                                                         | 13 |
| Recommendations.....                                                                                  | 21 |
| Introduction .....                                                                                    | 26 |
| Background to the review .....                                                                        | 26 |
| Context.....                                                                                          | 26 |
| Methodology.....                                                                                      | 27 |
| What are online harms and how are they relevant to children in Jersey? .....                          | 28 |
| Defining “online harms” .....                                                                         | 28 |
| Are children and young people considered to be more vulnerable to potential online harms? .....       | 32 |
| Impact of online harms on children in Jersey .....                                                    | 36 |
| Legacy of the Independent Jersey Care Inquiry.....                                                    | 40 |
| What are children’s rights in the digital environment? .....                                          | 42 |
| Why did Jersey reject the option of a permissive extent clause to the U.K.’s Online Safety Act? ..... | 45 |
| What is a permissive extent clause? .....                                                             | 45 |
| How was the decision about the OSA PEC made? .....                                                    | 46 |
| How will Jersey internet users be classified? .....                                                   | 51 |
| Alignment with other jurisdictions, including the Crown Dependencies.....                             | 53 |
| PEC process summary .....                                                                             | 54 |
| How are children in Jersey currently protected from types of online harm? .....                       | 56 |
| Legislation .....                                                                                     | 56 |
| Policy .....                                                                                          | 62 |
| Internet Service Providers .....                                                                      | 65 |
| Platforms’ own rules and guidelines .....                                                             | 68 |
| During school time.....                                                                               | 70 |
| Youth clubs .....                                                                                     | 81 |
| Children in the care of the Minister .....                                                            | 82 |
| Corporate Parents.....                                                                                | 83 |
| Cybersecurity .....                                                                                   | 84 |
| Provision of support.....                                                                             | 85 |
| Types of Online Harm.....                                                                             | 86 |

|                                                                                         |     |
|-----------------------------------------------------------------------------------------|-----|
| Child Sexual Abuse.....                                                                 | 86  |
| Exposure to harmful or inappropriate content, including suicide and self-harm .....     | 88  |
| Online grooming, harassment or stalking .....                                           | 95  |
| Cyberbullying .....                                                                     | 98  |
| Financial Harms .....                                                                   | 101 |
| Privacy violations .....                                                                | 103 |
| Misinformation .....                                                                    | 107 |
| Harm to individual health.....                                                          | 109 |
| Who is responsible for prevention and protection of children from online harms? .....   | 112 |
| Parents, caregivers and family members .....                                            | 113 |
| Safety-by-Design .....                                                                  | 118 |
| Government led action .....                                                             | 119 |
| Role of Digital Platforms .....                                                         | 121 |
| What action can Jersey take to provide children with a safer digital future? .....      | 127 |
| Creation of an online safety strategy for Jersey .....                                  | 127 |
| Define expectations for digital skills.....                                             | 132 |
| Include views of the public, particularly co-design with children and young people .... | 136 |
| Clarify the role of Legislation .....                                                   | 138 |
| Clarify the role of data protection in relation to online harms .....                   | 144 |
| Improve Enforcement and Accountability .....                                            | 148 |
| Cross-Government coordination .....                                                     | 152 |
| School curriculum and CYPES online safety policy .....                                  | 155 |
| Ensure that there is support for children and young people impacted by online harm      | 157 |
| Engage businesses and digital platforms .....                                           | 160 |
| Other jurisdictions .....                                                               | 162 |
| Conclusion .....                                                                        | 164 |
| Appendix 1 .....                                                                        | 165 |
| Panel membership.....                                                                   | 165 |
| Terms of Reference.....                                                                 | 165 |
| Evidence considered .....                                                               | 165 |
| What is Scrutiny? .....                                                                 | 168 |

## Chair's Foreword

---



There is much research and evidence of the bad effects of the online world on children. Depression, anxiety, self-harm, radicalisation, exploitation, bullying... the list goes on. There is of course another side to it which is very positive – information sharing, learning, beneficial social networks, creative opportunities.

Back in 2024, the Children, Education and Home Affairs Scrutiny Panel (the 'Panel') discovered that, unlike the other Crown Dependencies, Jersey did not agree to be included in the UK's Online Safety Act. This decision was made by one Minister alone, with no consideration of children's rights or welfare, and was not even recorded as a ministerial decision. This is an important point, because even if you think that was the right decision, a matter which impacts children hugely should be a considered decision, including the relevant Ministers. What happened to the "putting children first" pledge? And it seems that the learnings from the Independent Jersey Care Inquiry have still not taken effect. I don't think the Minister was particularly to blame for this; it is the fault of Jersey's whole Government to not consider children's welfare across the board. Eight years after the publication of the report of the Independent Jersey Care Inquiry, there still appear to be systemic failings.

The Panel launched this review, which has included public hearings and many submissions. The result is this report, 63 findings and 38 recommendations. During this work, the Minister for Education and Lifelong Learning suggested there needed to be a conversation on this subject; well, this is it, and this can provide a basis for the Government to organise a detailed strategy. Other interested parties carried out their own studies – schools, the media, campaigners, and safeguarding organisations, which have all contributed to the conversation. The Ministers must respond thoughtfully to these recommendations; currently children in Jersey do not have the same protections as those in the UK, Ireland, and the rest of Europe, and that's not acceptable.

As well as the potential dangers online, such as sexual exploitation etc., the excessive use of screens is considered by many to be a public health crisis. During Panel visits to primary schools, headteachers have stated that one of the reasons for children being unprepared when starting school is excessive screen use. Children not knowing how to hold a crayon because, instead of playing, they've spent their early years on a screen. Or parents on their phones and not talking to their children.

In summary, online is "another world". The platforms have chosen to not prioritise children's welfare, so this is a world full of dangers to children. Jersey's stated Ministerial response is to create our own legislation. Whether this will have much effect in the international online world remains to be seen. And apart from the specific Violence Against Women and Girls recommended legislation, there is no child specific online safety legislation included in the legislative process. It does appear that when it comes to child safety and welfare Jersey is an outlier.

I would like to thank all those who contributed to this review, to the Panel members, and especially to the Panel officers.

**Deputy Catherine Curtis**  
**Chair,**  
**Children, Education and Home Affairs Scrutiny Panel**



## Executive Summary

---

This review examines Jersey's approach to online safety, with a particular focus on children and young people. It highlights the need for a coordinated, future-facing strategy that balances protection from harm with the preservation of digital rights. While digital access offers significant educational and social benefits, the Panel found that Jersey's current safeguards lag behind those of comparable jurisdictions, particularly in areas such as age verification, platform accountability, and cross-border enforcement.

### What is the relevance of 'online harms'?

The Children, Education and Home Affairs Scrutiny Panel (hereafter 'the Panel') found that while there is no universally accepted definition of "online harms," consistent terminology is essential for effective policy development. Online risks are not experienced equally, and children who are vulnerable offline are often more exposed in digital spaces. Jersey, despite its reputation as a safe environment, is not immune to global online threats, as evidenced by recent cases involving local children.

Emerging technologies like artificial intelligence require protective policy "guardrails" to balance innovation with ethical safeguards, especially for children. Although children themselves have not widely voiced concerns about online harms, parents and professionals have raised issues around screen time, smartphone use, and digital wellbeing (i.e. the state of a person's physical, mental and emotional health in relation to their use of digital technologies). Public health data suggests these patterns warrant further investigation.

### Permissive Extent Clause

The Panel examined Jersey's decision not to request a permissive extent clause ('PEC') for the U.K.'s Online Safety Act ('OSA') and found significant gaps in transparency, consultation, and legislative follow-up. The decision was made solely by the Minister for Sustainable Economic Development without formal documentation, engagement with the Council of Ministers, or States Assembly scrutiny. This lack of process limited opportunities for democratic oversight and public accountability.

Despite the OSA's central aim of protecting children online, no consultation took place with the Office of the Children's Commissioner or the Minister responsible for coordinating children's policy. The absence of such engagement raises concerns about the prioritisation of children's rights in digital policymaking and the extent to which lessons from the Independent Jersey Care Inquiry have been embedded in current governance.

The Panel also found no evidence that rejecting the PEC initiated any alternative legislative work to safeguard Jersey users. The Panel does not believe that Minister's assumptions that U.K. and E.U. regulations would indirectly protect Jersey residents are wholly correct, particularly in relation to age verification measures. As a result, children in Jersey may now face fewer barriers to accessing inappropriate content than their U.K. counterparts.

Jersey's position diverges from that of Guernsey and the Isle of Man, both of which requested permissive extent clauses for the Online Safety Act. Although neither jurisdiction has activated their PECs, Jersey's decision not to engage at all places it in a potentially anomalous and less protected position. The Panel has recommended that the Government of Jersey establish a formal process for considering PECs, including a requirement for Ministerial decisions and scrutiny. Additionally, a full assessment of the "umbrella effect" of U.K. and E.U. online safety

legislation should be conducted and published to ensure transparency and inform future policy development.

### Current protections

The Panel also explored the broader legislative and policy landscape surrounding online harms in Jersey and found that while some existing laws may offer limited protection, they do not comprehensively address the full spectrum of risks faced by children and young people in the digital environment. Ministers acknowledged the potential for future legislation, but concerns remain about enforcement capacity and the challenge of regulating global platforms from a small jurisdiction.

The development of legislation recommended by the Violence Against Women and Girls ('VAWG') Taskforce report presents an opportunity to address online harms, yet its current scope does not specifically focus on children, leaving a potential gap in protections. The Panel was advised that future legislation should adopt a technology-neutral approach, focusing on the nature of harm rather than the platform or tool, so that laws remain adaptable to emerging threats.

While various Government policies touch on aspects of online safety, there is no overarching framework connecting them. The Building a Safer Community framework has been suggested as a potential location for coordinating work related to online safety, but coordination between departments remains limited. Notably, the Department for the Economy had not collaborated with the Safeguarding Partnership Board, as its work had not been child focused. A cross-Ministerial group was established in late 2024 to consider Jersey's approach to online harms, supported by an officer group, but its terms of reference and progress have not yet been shared with Scrutiny.

Technical limitations also pose challenges. Internet Service Providers in Jersey cannot block certain harmful content, and users can bypass restrictions using Virtual Private Networks ('VPNs') and proxy IP addresses. Unlike the U.K.'s OSA, Jersey has no equivalent obligations for platforms to prevent children from circumventing safety measures. In the absence of government-defined standards, platform-led content governance, driven by corporate policies, has become the default, raising concerns about consistency and accountability.

In educational settings, schools play a dual role in safeguarding and educating children about online safety. However, the current CYPES Online Safety Policy, dated August 2021, is outdated and under review. Filtering and monitoring software only applies to devices connected to school networks, leaving gaps when students use mobile data. New restrictions on mobile phone use in schools were announced for September 2025, but the Panel has found that such measures may not address the root causes of harmful content and could limit access to digital learning.

It was confirmed to the Panel that online safety education is a statutory responsibility and embedded in the Jersey curriculum, though funding is limited and training is often school led. Schools face challenges in delivering age-appropriate and SEN-sensitive content. Also, the Minister for Children and Families has stated that there is no need to oversee and monitor the use of technology when attending a youth centre as the Jersey Youth Service does not currently provide any devices for children and young people to access the internet. The Panel is concerned that the absence of provided devices does not remove the duty of care owed by youth services when children are in their care.

The Panel also found that the CYPES Online Safety Policy does not apply to the Children's Residential Service, however, residents are provided with internet usage rules and individual care plans to manage vulnerabilities. A comprehensive policy review is underway. The Residential Service uses Sophos software to monitor and filter harmful content on connected devices; however, filtering was not in place at the two Children's Short Breaks Homes. This gap was acknowledged and is expected to be addressed. The Panel has recommended that the planned updates to Children's Services policies include clear provisions for online safety, with specific measures to mitigate risks associated with mobile data access for looked-after children.

The Panel has also recommended amending the Protection of Children (Jersey) Law 1994 to ensure that all individuals under the age of 18 are uniformly protected, including in provisions relating to indecent photographs, following evidence provided to the Panel by the States of Jersey Police.

### Types of Harm

While Jersey has legislation criminalising the creation and distribution of child sexual abuse material (CSAM), and a multi-agency strategy on Child Sexual Abuse and Exploitation (CSAE), broader protections against harmful online content remain limited. The Panel recommends developing legislation that mandates platforms to monitor or remove inappropriate digital content, such as material encouraging suicide or self-harm. It also urges the cross-Ministerial group to coordinate with Public Health and align efforts with the "Connected in Hope" suicide prevention strategy.

Online or digital age-verification measures are not currently mandated in Jersey, and Ministers have expressed concerns about privacy and effectiveness. The Panel recommends evaluating age assurance systems used in other jurisdictions to assess their potential benefits and risks for local adoption. Additionally, the Panel suggests reviewing the Sexual Offences (Jersey) Law 2018 to consider whether misrepresentation by adults to minors, such as falsifying age or identity, should be criminalised.

In education settings, the Panel has recommended that the CYPES Counter Bullying Policy should be updated to provide clearer guidance on responding to cyberbullying, including incidents that may involve criminal behaviour, while ensuring children are safeguarded without being unnecessarily criminalised. It also recommends assessing whether Jersey users benefit from platform design changes introduced elsewhere, particularly those aimed at reducing manipulative features and exposure to unsafe digital environments.

The amplification of false or misleading content through algorithmic systems was identified as a growing risk to public safety. The Panel noted that the Government has no plans to introduce specific measures to tackle misinformation online, however, recommends that the Ministerial and Officer groups reviewing online safety policy assess how Jersey intends to respond to algorithmically accelerated misinformation. Furthermore, the Panel encourages collaboration with Public Health Jersey to incorporate evidence-based guidance on screen time into education and children's services policies.

### Who is responsible?

The Panel was advised that protecting children from online harm requires a whole-of-society approach, involving coordinated efforts across government departments, education, health, law enforcement, and the private sector. While there is consensus on the need for collaboration, a key challenge lies in defining the scope of Jersey's response, whether it should



be locally tailored or aligned with broader international regulatory frameworks. The Panel emphasised that any strategy must reflect Jersey's unique context while remaining informed by global standards and best practice.

Promoting healthy alternatives to screen time was identified as a vital component of digital wellbeing. Public Health Jersey has recommended expanding access to free, inclusive activities such as sport, arts, and community programmes to encourage physical activity, creativity, and social engagement. The Panel supports this approach and recommends that the draft Play Strategy explicitly consider how government initiatives can provide young people with meaningful substitutes to screen-based entertainment.

A persistent challenge is the lag between rapid technological innovation and the implementation of effective safeguards. The Panel found that digital platforms should bear greater responsibility for designing services that are safe and developmentally appropriate for children. This includes addressing addictive design features and ensuring systems are in place to detect and respond to harmful behaviours. While some platforms may anticipate regulation and adopt voluntary standards, the UN Convention on the Rights of the Child (UNCRC) affirms that it is the role of governments, not corporations, to set and enforce standards that protect children's rights in digital environments. The Panel recommends that the Government of Jersey initiate policy development to explore legislative approaches that place greater accountability on digital platforms, ensuring their operations are guided by principles of safety and rights by design.

#### What next?

The Panel recommends that the development of a comprehensive online safety strategy is essential to safeguarding children and supporting digital wellbeing across Jersey. Ministers have expressed support for such a strategy, and the cross-Ministerial group has indicated its intention to begin coordinating this work. However, the Panel is concerned that significant long-term action may not be initiated within the remainder of the current political term. It recommends that the Government prioritise the creation of a forward-looking, rights-based strategy that incorporates cross-government collaboration and remains adaptable to evolving digital threats.

Digital education is acknowledged as a priority, yet there is a lack of clear guidance on what constitutes digital literacy. While many children are proficient in using devices and platforms, this does not equate to true digital literacy or responsible digital citizenship. The Panel recommends that the Government define these concepts for all Islanders as part of its strategy and embed them into lifelong learning ambitions, with targeted support for adults to help guide children's digital development.

Digital literacy and online safety must be embedded into education systems and supported by investment in infrastructure, teacher training, and evidence-based standards. The Panel recommends ensuring equitable access to digital education across all schools.

To shape an effective strategy, the Government must understand how children and young people engage with the internet and what they perceive as harmful. The Panel recommends conducting research to inform policy and ensure legislation addresses the full spectrum of digital harms, including those emerging from new technologies.

While updates to existing laws, particularly those linked to data protection and the VAWG report, are underway, these efforts do not comprehensively address the wide-ranging nature of online harms. Stakeholders such as the NSPCC, Safeguarding Partnership, and

Information Commissioner have stressed the need for regulatory alignment and forward-looking legislation. The Panel advises that Jersey's legislative strategy clearly distinguish between privacy protections and broader online harms, rather than relying solely on data protection law.

The Jersey Office of the Information Commissioner (JOIC) has been suggested as a potential regulator for online safety initiatives. However, JOIC is not currently resourced for this role. The Panel recommends a formal capacity assessment and consideration of alternative regulatory models, including partnerships with other jurisdictions.

Responsibility for the digital economy currently sits with the Minister for Sustainable Economic Development, while the Minister for Children and Families has responsibility for coordinating policies to safeguard children and support children's wellbeing. Given the centrality of child protection to online safety, the Panel recommends assigning Ministerial responsibility for this area to the Minister for Children and Families.

Finally, the Panel highlights the importance of establishing clear, child-friendly reporting pathways for online harm. Data from the Jersey Children and Young People's Survey indicates that some young people are hesitant to report experiences of exploitation. The Panel recommends developing a simple, accessible system for reporting harmful online content, supported by community learning initiatives that empower children, parents, and professionals to respond effectively.

## Findings and Recommendations

---

As part of this review, the Panel has identified 63 findings and put forward 38 recommendations. While all are considered significant in shaping the understanding and context of child protection within Jersey's online environment, the Panel has chosen to highlight 6 findings and 5 recommendations as key points. These are as follows:

### Key Findings

#### **FINDING 4**

Although Jersey has been typically regarded as a safe environment for children, it remains vulnerable to the risks associated with the online world. The borderless nature of digital spaces means that children and young people in the Island can be exposed to harmful content and influences originating from anywhere in the world. A recent court ruling has brought to light a case involving the exploitation of local children where communications have been facilitated by online platforms.

#### **FINDING 6**

Issues around smartphone and screen use have been highlighted to the Panel by members of the public and through locally collected data. Public Health has referenced data in the Jersey Children and Young People's Survey and has suggested that emerging patterns warrant deeper investigation to better understand the health impacts of screen use and inform policy development in Jersey.

#### **FINDING 7**

No assessment of children's rights was undertaken as part of the analysis of the option of a permissive extent clause for Jersey in the U.K.'s Online Safety Act, despite the legislation's purpose to improve online safety for children. The Panel is concerned that this demonstrates that the lessons and recommendations from the Independent Jersey Care Inquiry (for example, ensuring that the interests of children are paramount and that legislation does not lag behind other jurisdictions) are not widely embedded into practice across the whole of Government.

#### **FINDING 14**

In May 2025, the Minister for Sustainable Economic Development informed the Panel that regulatory changes in the U.K. and Europe might create an "*umbrella effect*" for Jersey users. Specifically, if the U.K. introduced age verification for certain websites, Jersey users would likely need to comply with the U.K.'s system. However, when the Panel informally tested this assumption in July 2025, after the U.K.'s child safety provisions took effect, it was found that Jersey was not covered by the age verification changes. Therefore, children in Jersey may now face fewer barriers, compared to their counterparts in the U.K., when attempting to access content that is not considered age appropriate.

#### **FINDING 26**

The absence of government-defined standards or regulations in Jersey for platform-led content governance suggests an implicit acceptance that decisions about potentially harmful content, particularly affecting children, are determined by corporate policies rather than by local legislative oversight or public authority.

#### **FINDING 54**

A key challenge is the lag between technological innovation and the implementation of effective safeguards for online safety. The Panel's review has gathered evidence indicating that digital platforms should bear greater responsibility for designing their services to be suitable and safe for children, including addressing addictive behaviours and identifying and flagging inappropriate online behaviour. Whilst some platforms may anticipate regulatory demands and "self-regulate" the

UNCRC has made it clear that it is the role of governments to set the standards for a safe digital environment that is in the best interests of children.

## Key Recommendations

### **RECOMMENDATION 4**

Policy considerations should be subject to a formal assessment of children's rights at an early stage. The Government of Jersey should evidence how it will embed this process across all departments to reflect the enduring lessons of the Independent Jersey Care Inquiry.

### **RECOMMENDATION 7**

The Government of Jersey should conduct and publish a comprehensive gap analysis of existing legislation addressing online harms, with particular attention to the range of types of harm currently covered. This analysis should also consider the absence of child-specific protections in emerging frameworks such as the VAWG legislation and reflect the enforcement challenges faced by a small jurisdiction operating in a global digital environment.

### **RECOMMENDATION 10**

The Minister for Sustainable Economic Development should explore and undertake a public consultation on the development of legislation that would require all on-Island internet service providers to introduce network-level filtering that is active by default and customisable by the contract holder.

### **RECOMMENDATION 26**

The Minister for Children and Families and Minister for Education and Lifelong Learning should engage with Public Health Jersey to explore how evidence-based guidance on screen time can be incorporated into government policy and translated into updated practical measures within education and children's services.

### **RECOMMENDATION 29**

The Government of Jersey should prioritise the development of a comprehensive online safety strategy, with a particular emphasis on safeguarding children. Such a strategy should be grounded in a rights-based framework, incorporate cross-government collaboration, be forward-looking, and capable of addressing current challenges while remaining adaptable to the evolving digital environment.

## Findings

### **FINDING 1**

There is currently no internationally recognised definition for “online harms” however, a range of shared classifications and terminology has emerged. Establishing consistent language and definitions is important for improving understanding and addressing the complexities of online harms.

### **FINDING 2**

Online harms are not experienced equally and in order to address risks it is important to understand *who* is harmed and *how*. Online risks can reflect or intensify the dangers children face offline, with those already vulnerable in real-world settings more likely to be at risk in digital spaces.

### **FINDING 3**

Protective measures or “guardrails” can be used in policy and legislation development in relation to technology developments, such as A.I. and other emerging digital tools. These safeguards help ensure that innovation is balanced with ethical considerations, user safety, and the protection of fundamental rights, particularly for vulnerable groups such as children and young people.

### **FINDING 4: Key Finding**

Although Jersey has been typically regarded as a safe environment for children, it remains vulnerable to the risks associated with the online world. The borderless nature of digital spaces means that children and young people in the Island can be exposed to harmful content and influences originating from anywhere in the world. A recent court ruling has brought to light a case involving the exploitation of local children where communications have been facilitated by online platforms.

### **FINDING 5**

Digital safety or online harms is not an issue that has been raised as a worry or concern by children themselves with the Children’s Commissioner for Jersey, or the Minister for Children and Families. Instead, issues affecting children’s health and safety online are more often voiced by parents and other adults.

### **FINDING 6: Key Finding**

Issues around smartphone and screen use have been highlighted to the Panel by members of the public and through locally collected data. Public Health has referenced data in the Jersey Children and Young People’s Survey and has suggested that emerging patterns warrant deeper investigation to better understand the health impacts of screen use and inform policy development in Jersey.

### **FINDING 7: Key Finding**

No assessment of children’s rights was undertaken as part of the analysis of the option of a permissive extent clause for Jersey in the U.K.’s Online Safety Act, despite the legislation’s purpose to improve online safety for children. The Panel is concerned that this demonstrates that the lessons and recommendations from the Independent Jersey Care Inquiry (for example, ensuring that the interests of children are paramount and that legislation does not lag behind other jurisdictions) are not widely embedded into practice across the whole of Government.

#### **FINDING 8**

The United Nations Convention on the Rights of the Child (UNCRC) Rights are equally applicable to children in the digital environment, and all rights must be considered equally. A tailored approach is essential and there is no one-size-fits-all solution when safeguarding children's rights online.

#### **FINDING 9**

There is a requirement for the States Assembly to approve the extension of any U.K. Act to Jersey, however, there is no formal process or requirement for permissive extent clauses which are offered for Jersey to be discussed by the States Assembly or Council of Ministers, and the decision making power as to whether to reject them lies with the Minister who is deemed to have political responsibility for the relevant area in question. To ensure greater transparency, future decisions should involve clearer information sharing with both the Council of Ministers and Scrutiny.

#### **FINDING 10**

The decision not to request a permissive extent clause for Jersey in the U.K.'s Online Safety Act was made solely by the Minister for Sustainable Economic Development during the period September – November 2022. The reasoning given for this was that the U.K.'s Online Safety Act was considered to be an overly complex "poor" law, a "tick-box exercise" and, because of the principle that Jersey should legislate for itself.

#### **FINDING 11**

The Minister for Sustainable Economic Development's decision was not recorded in a formal Ministerial decision or shared with the Council of Ministers so there was no opportunity for scrutiny and no transparent decision-making process.

#### **FINDING 12**

The Minister for Sustainable Economic Development did not consult the Office of the Children's Commissioner, or the Minister with responsibility for coordinating polices relating to children despite the fact that a central aims of the U.K.'s Online Safety Act is to ensure that children receive a higher level of protection from potential harms associated with internet services.

#### **FINDING 13**

There is no evidence that the Minister for Sustainable Economic Development's decision to reject the permissive extent clause for the U.K.'s Online Safety Act in late 2022, initiated any alternative work to assess how local legislation could be developed to provide alternative protection for users in Jersey.

#### **FINDING 14: Key Finding**

In May 2025, the Minister for Sustainable Economic Development informed the Panel that regulatory changes in the U.K. and Europe might create an "*umbrella effect*" for Jersey users. Specifically, if the U.K. introduced age verification for certain websites, Jersey users would likely need to comply with the U.K.'s system. However, when the Panel informally tested this assumption in July 2025, after the U.K.'s child safety provisions took effect, it was found that Jersey was not covered by the age verification changes. Therefore, children in Jersey may now face fewer barriers, compared to their counterparts in the U.K., when attempting to access content that is not considered age appropriate.

#### **FINDING 15**

Jersey is a potential anomaly compared to the other Crown Dependencies of Guernsey and the Isle of Man, which both opted to request a permissive extent clause be included the U.K.'s



Online Safety Act. However, the Panel was advised in May 2025 that neither of the other Crown Dependencies had 'activated' its permissive extent clause.

#### **FINDING 16**

Ministers advised that existing legislation in Jersey may offer some protection against online harms. However, the scope of this legislation appears to be disjointed, addressing only certain types of harm and lacking comprehensive coverage of the full range of risks children and young people face in the digital environment.

#### **FINDING 17**

Ministers have indicated that further legislation could be developed to enhance protections against online harms. However, concerns remain regarding the practical challenges of enforcement, particularly given Jersey's position as a small jurisdiction. The Panel also noted the complexities of legislating independently on an issue that is inherently international in nature, where influence over global digital platforms may be limited.

#### **FINDING 18**

The Violence Against Women and Girls (VAWG) legislation currently in development offers an opportunity to address online harms. However, its scope does not specifically focus on children, which potentially leaves a gap in protections for young people in the digital environment.

#### **FINDING 19**

The Panel was advised that any legislation aimed at providing protection should focus on the harm itself rather than the technology through which it occurs. A technology neutral approach ensures laws remain effective as new digital threats emerge, while technology-specific laws risk becoming outdated.

#### **FINDING 20**

Various Government policies play a role in addressing elements of online safety and providing protection from online harm but there is not an established interconnection between them. It has been suggested that the Building a Safer Community framework could be used to coordinate work.

#### **FINDING 21**

The Department for the Economy has not had any collaboration with the Safeguarding Partnership Board in relation to their work about online harms, as its work had not been focussed on children.

#### **FINDING 22**

A cross-Ministerial group was created in September / October 2024 to consider the Government of Jersey's approach to protection against online harms, however, no Chair had been appointed as of May 2025. The Panel also learned that an officer group would be established to support this work.

#### **FINDING 23**

Internet Service Providers in Jersey cannot block content on various websites, therefore internet users in Jersey may be able to access content that would be blocked by networks in the U.K.

#### **FINDING 24**

Virtual Private Networks (VPNs) and proxy internet protocol (IP) addresses create further challenges for enforcing jurisdictional boundaries on the internet as users can circumnavigate restrictions from the region they are in. In the U.K. the Online Safety Act creates obligations

for platforms to prevent children bypassing safety precautions, but there is no equivalent obligation in Jersey legislation.

#### **FINDING 25**

Social media and online platforms typically enforce 'terms of service' or 'community guidelines' that users must follow to maintain access and help ensure a safer, more respectful environment for everyone, however, each platform or company will define its own unique set of rules which leads to different standards across platforms. Whilst TikTok has confirmed that it has a global approach and that users in Jersey receive the same user experience as those in other jurisdictions, this is not the same for every social media or digital platform.

#### **FINDING 26: Key Finding**

The absence of government-defined standards or regulations in Jersey for platform-led content governance suggests an implicit acceptance that decisions about potentially harmful content, particularly affecting children, are determined by corporate policies rather than by local legislative oversight or public authority.

#### **FINDING 27**

Schools serve a dual role in relation to protecting children from online harms: to safeguard students and, also, educate them about how to stay safe online. The Minister for Education and Lifelong Learning also advised that schools had to work with parents and had been “drawn in” to the world of mobile phones.

#### **FINDING 28**

School statutory responsibilities for safeguarding are set out in Appendix 5 of the School Review Handbook and this includes responsibilities related to online harms. School reviews under the School Review Framework are conducted every 3-4 years.

#### **FINDING 29**

The current CYPES Online Safety Policy is dated August 2021 and the Panel established that several aspects detailed within it are no longer operational practice. It was confirmed that procedures have since been updated and improved, and that the policy itself is undergoing review. The Panel was advised that a revised version will be published to align with the updates.

#### **FINDING 30**

The Online Safety Policy and safety features such as filtering and monitoring software are only applicable to devices that are connected to the school network or wi-fi. If an individual uses data on a mobile device to access the internet, the CYPES filtering software will not apply.

#### **FINDING 31**

During the course of the review, the Minister for Education and Lifelong Learning announced that there would be more restrictions put in place for students' use of mobile phones within all Government provided and fee-paying schools from September 2025.

#### **FINDING 32**

Restrictions or bans on mobile phone use in educational settings can be a way to reduce potential risks, such as exposure to inappropriate content and excessive screen time. However, these measures do not address the root causes related to harmful content itself and may inadvertently limit students' access to educational resources and opportunities to develop essential digital skills.

### **FINDING 33**

Education about online safety and protection from online harms is a statutory responsibility for schools and is incorporated within the Jersey curriculum in both primary and secondary schools and some schools have also developed their own digital literacy programmes. However, there is no dedicated budget for online safety training in schools. A sum of £6,000 was allocated from the central CYPES training budget, with additional training for teachers funded directly by schools. The Minister has highlighted peer learning among staff as a valuable resource.

### **FINDING 34**

There are challenges in delivering age-appropriate and SEN-sensitive online safety education, with schools reportedly tailoring approaches to individual pupil needs.

### **FINDING 35**

The Minister for Children and Families has stated that there is no need to oversee and monitor the use of technology when attending a youth centre as the Jersey Youth Service does not currently provide any devices for children and young people to access the internet. The Panel is concerned that the absence of provided devices does not remove the duty of care owed by youth services when children are in their care.

### **FINDING 36**

The CYPES Online Safety Policy does not apply to the Children's Residential Service, however, residents are provided with internet usage rules and expectations, and individual care plans and safety strategies are used to manage vulnerabilities and safeguard against online harm. The Panel was informed that Children's Services is undertaking a comprehensive policy review.

### **FINDING 37**

The Residential Service uses a system called Sophos to monitor wi-fi use and filter or block harmful content from any device connected to the wi-fi, however, the Panel found that internet filtering software was not in place at the two Children's Short Breaks Homes. It was confirmed in May 2025 that this would be addressed and implemented at those locations in the near future.

### **FINDING 38**

The Cyber Security (Jersey) Law is a resilience law with the purpose of ensuring the safety of the Island's digital infrastructure and providing online safety to citizens as a consequence of this. It is not a law that is designed to provide any protection for children from content on the internet.

### **FINDING 39**

In Jersey, there is legislation that makes the creation or distribution of child sexual abuse material (CSAM) a criminal offence. There is also a multi-agency [strategy on Child Sexual Abuse and Exploitation \(CSAE\)](#) published by the Safeguarding Partnership Board. Where CSAM is found, it can be reported to the Internet Watch Foundation who will work internationally to remove the content from the internet. There are plans to make amendments to the Sexual Offences (Jersey) Law 2018 to address non-consensual sharing of sexual images.

### **FINDING 40**

There is legislation that makes it illegal to aide, abet, counsel or procure a person's suicide, however, unlike the United Kingdom, Jersey does not have legislation that mandates online platforms or service providers to monitor or remove inappropriate digital content, including

suicide related content and self-harm material, or to implement age-assurance measures for accessing certain material and the Panel has established that no work is being progressed to address this.

#### **FINDING 41**

The Panel notes that within the current legislative framework, the concept of “take down requests” has predominantly been considered in the context of proposed amendments to data protection legislation. These measures are intended to tackle online harms involving personal data and are unlikely to apply to wider content reporting mechanisms, especially where the material does not directly concern the personal information of the individual making the report. In such cases, platform-specific guidelines are more likely to govern how the content is handled.

#### **FINDING 42**

The Government of Jersey has committed to implementing all Violence Against Women and Girls Taskforce recommendations, including regulating online platforms (Recommendation 10). However, current efforts by the Government focus solely on removing harmful content targeting individuals, without broader measures to regulate content.

#### **FINDING 43**

The Government of Jersey currently has no plans to introduce regulations requiring service providers to implement age-verification measures for users accessing specific online content, such as pornography. Ministers have been critical of age-verification measures. The Minister for Sustainable Economic Development has stated that requirements to provide age verification are not considered appropriate for Jersey citizens, as it involves individuals disclosing highly sensitive personal information to third parties. Additionally, it may create a misleading impression of online safety, given that age-verification measures can be easily circumvented, for instance, using a VPN.

#### **FINDING 44**

Cyberstalking will be addressed within the scope of the legislation that is being developed in response to the Violence Against Women and Girls Taskforce Report recommendations and is expected to be lodged within the existing electoral term (to June 2026).

#### **FINDING 45**

Article 51 of the Telecommunications (Jersey) Law 2002 makes the improper use of a telecommunications system an offence. However, it does not establish the same level of responsibility as the U.K.’s Online Safety Act, which places explicit duties on digital platforms, for example, to implement safeguards against harmful content, conduct regular risk assessments, and ensure systems are in place to prevent and respond to behaviours such as cyberbullying, harassment, and online abuse.

#### **FINDING 46**

The Government of Jersey is developing a centralised database to collect data on technology-facilitated abuse, including cyberbullying, cyberstalking, non-consensual intimate image abuse, online gender-based hate speech, and cyberharassment.

#### **FINDING 47**

Prosecuting against online financial harms, such as fraud, is challenging when the perpetrator is not in Jersey and is in another jurisdiction as it makes pursuing criminal action more difficult. It is unclear whether internet users in Jersey will benefit from platform design changes in other jurisdictions.

#### **FINDING 48**

Minimum age requirements for information society services (e.g. social media platforms) are primarily derived from data protection legislation, rather than assessments of children's developmental readiness or online safety needs.

#### **FINDING 49**

The Government of Jersey has indicated that it will develop legislation to further extend the rights of data subjects, including children. However, in order to remain aligned with the EU's GDPR legislation it will not extend to individuals acting in a personal or household capacity, due to the domestic purpose exemption. As a result, data protection legislation will not adequately address the full spectrum of online harms, particularly those arising from personal content sharing or harmful behaviour between individuals online.

#### **FINDING 50**

The impact of false or misleading content, particularly when amplified by algorithms, has been found to be a risk to public safety in the U.K. In Jersey, the Minister for Sustainable Economic Development has confirmed that there are no government plans to introduce specific measures aimed at tackling misinformation online.

#### **FINDING 51**

State parties should proactively consider emerging research and evidence from the public health sector to help prevent the spread of misinformation, as well as materials and services that may harm children's mental or physical health. Such action would support the Government's obligations under the United Nations Convention on the Rights of the Child (UNCRC).

#### **FINDING 52**

There is a consensus that protecting children from online harm requires a societal approach, involving collaboration across multiple sectors. However, a key challenge includes defining the scope of the response, particularly whether it should be locally tailored to Jersey or aligned with international regulatory frameworks.

#### **FINDING 53**

Enticing alternatives to screen time are important to encourage physical activity, creativity, and social engagement. Public Health Jersey has recommended improving access to free, inclusive activities, such as sport, arts, and community programmes, as a means to offer positive substitutes to screen time.

#### **FINDING 54: Key Finding**

A key challenge is the lag between technological innovation and the implementation of effective safeguards for online safety. The Panel's review has gathered evidence indicating that digital platforms should bear greater responsibility for designing their services to be suitable and safe for children, including addressing addictive behaviours and identifying and flagging inappropriate online behaviour. Whilst some platforms may anticipate regulatory demands and "self-regulate" the UNCRC has made it clear that it is the role of governments to set the standards for a safe digital environment that is in the best interests of children.

#### **FINDING 55**

Ministers have expressed support for the development of an online safety strategy, and the Panel has been informed that the cross-Ministerial group intends to begin coordinating this work. However, based on current indications, the Panel understands that significant long-term action may not be initiated within the remainder of the current political term.

#### **FINDING 56**

The Government of Jersey has acknowledged the significance of digital education, yet there remains a lack of clear guidance around defining digital literacy expectations. While many children are proficient in using digital devices and platforms, this competence does not automatically translate into true digital literacy.

#### **FINDING 57**

Government of Jersey Ministers have indicated that they are introducing new legislation on online harms, however, the evidence presented to the Panel has largely focused on updates to existing laws and ongoing initiatives linked to data protection and the VAWG report. However, these efforts alone do not comprehensively address the wide-ranging nature of online harms.

#### **FINDING 58**

The Panel has heard that any new or updated legislation must be forward looking and that there should be regulatory alignment to enable cross-border enforcement and ensure child-specific protections. While Ministers value legislative autonomy, stakeholders including the NSPCC, Safeguarding Partnership Board, and Information Commissioner stressed that fragmented or reactive laws risk being ineffective.

#### **FINDING 59**

Data protection law is critical for privacy and supporting user rights but cannot address the full spectrum of online harms. Government of Jersey Ministers have cited the importance of ensuring that Jersey's data protection laws maintain adequacy and continue to align with the EU's General Data Protection Regulation (GDPR).

#### **FINDING 60**

The Minister for Sustainable Economic Development has suggested that the Jersey Office of the Information Commissioner (JOIC) could potentially lead enforcement efforts for the Government's planned online safety initiatives. However, JOIC is not presently resourced to serve as the regulator, and expanding its role would necessitate substantial investment.

#### **FINDING 61**

Responsibility for the digital economy in Jersey currently sits with the Department for the Economy and the Minister for Sustainable Economic Development, while the Minister for Children and Families holds formal responsibility for coordinating policies to safeguard children and support their well-being.

#### **FINDING 62**

Digital literacy and online safety need to be embedded into education systems and keep up with technological change. The UNCRC has advised that equitable investment in infrastructure, teacher training, and evidence-based standards to ensure ethical and educational use of technology.

#### **FINDING 63**

Data from the Jersey Children and Young People's Survey suggests that some young people are hesitant to report experiences of criminal or sexual exploitation. While not all such harm occurs online, the data underscores the importance of establishing clear, accessible reporting pathways and support systems to safeguard children in digital spaces.



## Recommendations

### **RECOMMENDATION 1**

The Government of Jersey should ensure that any further work initiatives to address risks related to online harms include clear definitions and classification of the specific types of harm being targeted. This will help to facilitate a shared understanding between different groups of stakeholders and, where applicable, support alignment across jurisdictions.

### **RECOMMENDATION 2**

The Minister for Children and Families should coordinate work to assess the risks and impact of different online harms to all children and identify vulnerable groups in order to develop targeted interventions. This work would inform policy decisions and ensure that safeguarding measures are inclusive, evidence based and responsive to emerging threats.

### **RECOMMENDATION 3**

The Government of Jersey should explore the development of policy and legislative guardrails to ensure the safe, ethical, and responsible use of artificial intelligence across public and private sectors. The guardrails should be designed for all users but consider special protections for children.

### **RECOMMENDATION 4: Key Recommendation**

Policy considerations should be subject to a formal assessment of children's rights at an early stage. The Government of Jersey should evidence how it will embed this process across all departments to reflect the enduring lessons of the Independent Jersey Care Inquiry.

### **RECOMMENDATION 5**

The Government of Jersey should create a formal process which widens the scrutiny available to the option of a permissive extent clause prior to the decision being made. As a minimum a Ministerial decision should be required, so that the relevant Scrutiny Panel and members of the States Assembly and general public have the opportunity to raise questions.

### **RECOMMENDATION 6**

The Government of Jersey should formally research and assess what "umbrella" effect, if any, there is for Jersey internet users from the U.K.'s Online Safety Act and the EU's Digital Services Act. Assessment findings should be published for public transparency.

### **RECOMMENDATION 7: Key Recommendation**

The Government of Jersey should conduct and publish a comprehensive gap analysis of existing legislation addressing online harms, with particular attention to the range of types of harm currently covered. This analysis should also consider the absence of child-specific protections in emerging frameworks such as the VAWG legislation and reflect the enforcement challenges faced by a small jurisdiction operating in a global digital environment.



### **RECOMMENDATION 8**

The Government of Jersey should review its procedures to ensure that all Government departments are taking consideration of the impact of their work on children, as an automatic and integrated part of the policy development process.

### **RECOMMENDATION 9**

The Cross-Ministerial group should publish its terms of reference and provide details to scrutiny about the work it is doing to align relevant policies, data collection efforts, and governance frameworks to demonstrate that there is a coordinated approach to strategic planning and effective oversight to safeguard children and young people from online harms.

### **RECOMMENDATION 10: Key Recommendation**

The Minister for Sustainable Economic Development should explore and undertake a public consultation on the development of legislation that would require all on-Island internet service providers to introduce network-level filtering that is active by default and customisable by the contract holder.

### **RECOMMENDATION 11**

The Government of Jersey should clarify its position on legislating for online content governance, with particular emphasis on material that may be harmful to children. Doing so would signal whether the Island intends to establish its own regulatory standards or continue to rely on platform-led policies.

### **RECOMMENDATION 12**

The Minister for Education and Lifelong Learning and Minister for Children and Families should ensure the timely publication of the updated CYPES Online Safety Policy and share it with the Scrutiny Panel at the earliest opportunity to facilitate informed discussion and review. The revised Policy should explicitly address the appropriate access to online and digital content for children and young people attending school and educational settings, including the risks associated with mobile data use.

### **RECOMMENDATION 13**

The Minister for Education and Lifelong Learning should evaluate whether the U.K. based online safety guidance referred to in Jersey's Keeping Children Safe in Education policy suitably reflects Jersey's regulatory environment. Given the reliance on U.K.-based resources, and the potential divergence following the U.K.'s Online Safety Act, Jersey-specific measures should be developed to maintain effective protection for internet users.

### **RECOMMENDATION 14**

The Minister for Education and Lifelong Learning should engage with key stakeholders to review mobile phone policies and guidance for schools and, also, develop mechanisms to evaluate the effectiveness of the policy changes, ensuring they achieve their intended outcomes and provide meaningful protection for children in practice.

### **RECOMMENDATION 15**

The Minister for Education and Lifelong Learning should prioritise consistency in the delivery of online safety education across all schools with consideration about the suitability of funding for this statutory requirement. This includes ensuring that

teacher training is standardised and aligned with the digital education strategy to provide equitable learning experiences. Additionally, particular attention should be given to the development of tailored approaches for students with Special Educational Needs.

#### **RECOMMENDATION 16**

The Minister for Children and Families should ensure that any revised CYPES Online Safety Policy explicitly addresses the appropriate access to online and digital content for children and young people attending youth clubs, including the risks associated with mobile data use. This should be recognised as a distinct safeguarding responsibility within youth services.

#### **RECOMMENDATION 17**

The Minister for Children and Families should ensure that the updated policies for the Children's Services include clear provisions for online safety, with specific measures to mitigate risks associated with online harm and mobile data access for looked after children who are in the care of the Minister.

#### **RECOMMENDATION 18**

The Minister for Children and Families should amend the Protection of Children (Jersey) Law 1994 to ensure consistency in the definition of a child as any person under the age of 18. This revision should apply uniformly throughout the legislation, including provisions relating to indecent photographs, so that protections explicitly extend to all individuals under 18 years of age.

#### **RECOMMENDATION 19**

The Government of Jersey should develop legislation that mandates online platforms and service providers to monitor or remove inappropriate digital content, for example, content that encourages suicide or self-harm.

#### **RECOMMENDATION 20**

The Ministerial Group should seek specific guidance from Public Health in order to create coordination and joint working between the 'Connected in Hope: A strategy for Suicide Prevention in Jersey 2025-2029' and any work that the Government progresses in relation to online safety, for example under the Building a Safer Community framework.

#### **RECOMMENDATION 21**

The Government of Jersey should observe and evaluate age assurance measures introduced by other jurisdictions to determine their effectiveness in protecting children and consider the benefits and risks of adopting similar safeguards locally.

#### **RECOMMENDATION 22**

The Minister for Justice and Home Affairs should review the Sexual Offences (Jersey) Law 2018 to consider whether expanding offences about misinterpretation could provide additional protection for children in Jersey, for example, to make it specific offence for an adult to misrepresent their age, identity, sexual orientation, sex, or gender to a minor for the purposes of facilitating communication with that minor.

#### **RECOMMENDATION 23**

The CYPES Counter Bullying Policy should be updated to provide clear guidance for education settings on how to respond to and reduce cyberbullying, including

situations that may involve potentially criminal behaviour, while recognising the importance of safeguarding children without unnecessarily criminalising them.

#### **RECOMMENDATION 24**

The Government of Jersey should assess whether internet users in Jersey will benefit from platform design changes introduced in other jurisdictions to meet legal requirements, particularly those aimed at reducing manipulative design features and mitigating exposure to unsafe digital environments.

#### **RECOMMENDATION 25**

The Ministerial and Officer groups tasked with reviewing the online safety policy should give due consideration to the issue of algorithmically accelerated misinformation and assess whether, and in what manner, the Government of Jersey intends to respond to this in a local context. As larger jurisdictions have acknowledged, the amplification of false or misleading content through algorithmic systems can pose a risk to public safety, or wellbeing.

#### **RECOMMENDATION 26: Key Recommendation**

The Minister for Children and Families and Minister for Education and Lifelong Learning should engage with Public Health Jersey to explore how evidence-based guidance on screen time can be incorporated into government policy and translated into updated practical measures within education and children's services.

#### **RECOMMENDATION 27**

The Minister for Children and Families should ensure that the draft Play Strategy includes consideration of how the Government of Jersey could support initiatives that provide young people with a variety of free and inclusive alternatives to screen time.

#### **RECOMMENDATION 28**

The Government of Jersey should initiate policy development to explore effective legislative approaches that place greater accountability on digital platforms, ensuring their operations are guided by principles of safety and rights by design.

#### **RECOMMENDATION 29: Key Recommendation**

The Government of Jersey should prioritise the development of a comprehensive online safety strategy, with a particular emphasis on safeguarding children. Such a strategy should be grounded in a rights-based framework, incorporate cross-government collaboration, be forward-looking, and capable of addressing current challenges while remaining adaptable to the evolving digital environment.

#### **RECOMMENDATION 30**

As part of any future strategy development, the Government of Jersey should take steps to define 'digital literacy' and 'digital citizenship' and what these mean for all Islanders, in order to improve online safety and Jersey's digital culture.

#### **RECOMMENDATION 31**

The Minister for Education and Lifelong Learning should support digital literacy for all and make efforts to embed digital literacy into any lifelong learning ambitions for the Island. This includes targeted support for adults, in order to allow them to support children's digital development.

**RECOMMENDATION 32**

To shape an effective online safety strategy and understand the nature and impact of digital harms affecting children and young people, the Government of Jersey should research how children and young people engage with the internet and what they perceive as harmful within online environments.

**RECOMMENDATION 33**

The Government of Jersey's online safety strategy must reflect how any legislation will address the full spectrum of digital harms and be adaptable to emerging technologies and threats.

**RECOMMENDATION 34**

Jersey must clearly distinguish between data protection and protection from other online harms in its legislative strategy, ensuring that privacy safeguards are upheld without relying solely on data protection law to address the full spectrum of online harms.

**RECOMMENDATION 35**

Before assigning enforcement responsibilities for online safety legislation, the Government of Jersey should conduct a formal capacity assessment of the Jersey Office of the Information Commissioner (JOIC) and ensure that any expansion of its role is matched with appropriate funding, staffing, and statutory authority. Additionally, the Government should consider alternative regulatory approaches, including potential partnerships or agreements with other jurisdictions.

**RECOMMENDATION 36**

Ministerial responsibility for online safety should be assigned to the Minister for Children and Families, in recognition of the importance of safeguarding and child protection within this policy area.

**RECOMMENDATION 37**

The Minister for Education and Lifelong Learning should ensure that there is an equitable approach to online safety across schools and that investment is provided for technological infrastructure and resources that enable effective and inclusive digital education.

**RECOMMENDATION 38**

The Government should establish clear, child-friendly reporting pathways for online harm, supported by community learning initiatives that empower children, parents, and professionals to recognise and respond to exploitation. A simple, accessible system for Islanders to report harmful online content, accompanied by clear guidance on what to report, where to report it, and who handles it, should be developed.

## Introduction

---

### Background to the review

In October 2024 the Children, Education and Home Affairs Scrutiny Panel (hereafter, the 'Panel') held a public hearing with the Minister for Children and Families, the Minister for Justice and Home Affairs and the Minister for Sustainable Economic Development on the subject of 'Online Safety for Children in Jersey'.

The Panel had learned that the Government of Jersey had decided not to pursue a permissive extent clause ('PEC') for the United Kingdom's ('U.K.') Online Safety Act ('OSA') and wanted to gain an insight into the Government's decision-making process and how it could impact people, particularly children, using the internet in Jersey.

Other jurisdictions have taken legislative steps to put protection in place for citizens, especially children, from experiencing harm online. The OSA is the U.K.'s framework to improve and regulate certain internet services and digital communications. Legislation in other jurisdictions includes the European Union's Digital Services Act ('DSA') made by the European Commission, and the Online Safety and Media Regulation Act 2022 ('OSMR') in Ireland.

In October 2024, the Panel was advised that there was no existing internet safety strategy, but it was indicated that a cross-Government piece of work to develop one was possible. Following the hearing the Panel agreed to undertake this more formal review (subsequently launched in February 2025) in order to examine how Jersey was placed in terms of the various protection for online harms, through legislation, policy, or other means.

### Context

As this report will explore, the area of online harms is widespread and complex, and includes a range of issues ranging from misinformation and cyberbullying to data privacy and algorithmic bias, all of which can pose significant challenges to individuals and society. Online harms affecting children and young people is a concern for people worldwide, and the Panel had been contacted by Islanders who are worried, or have questions, about Jersey's position for ensuring online safety for children.

The past five years have brought substantial changes to the broader context and digital world. The Covid-19 pandemic in 2020 provided a catalyst to an already expanding world of technology and, for many, changed the intensity of use for digital and online services and technology. Furthermore, the way in which online tools are being used is also changing. In November 2022 OpenAI launched Chat GPT, the first generative artificial intelligence ('A.I.') chat-bot and it is suggested that this will be considered a key moment in the history of technology. Generative A.I. is expected to become more integrated into everyday life and is likely something that the Government of Jersey will need to address across various sectors, not just in relation to online harms.

In the U.K., the OSA, approved in 2023 has created a legal obligation for technology companies to protect children from harm when they are accessing websites and apps from the United Kingdom and there is protection provided by the DSA in the European Union and OSMR in Ireland.

Under the OSA, Ofcom has been granted powers as the online safety regulator of certain internet services for and in connection with communications offences and for connected purposes in the U.K., but this is not applicable in Jersey.

As part of this review, the Panel has sought to understand the steps taken by the Government of Jersey to develop its stance on the legislative framework for online child safety.

While some sectors and parents advocate for restricting children and young people's access to digital devices to shield them from online harms, there are others that emphasise the importance of retaining freedom of speech.

Just as physical play spaces have evolved to incorporate greater safety features with the advancement of health and safety standards, online environments, where children play, socialise, and grow, require thoughtful consideration. As the digital world becomes increasingly embedded in everyday life, it is essential to explore the implications this integration has for children and young people, and to identify the areas where Jersey's Government policy and action can support Islanders and keep children and young people safe online.

From the time of the Panel's standalone hearing in October last year, and this review's formal launch in early 2025, there have been a number of developments, for example, the Minister for Children and Families has voiced a commitment to an online safety strategy and the Minister for Education and Lifelong Learning has advised parents that there will be a change to further restrict smartphone use in Government provided schools from September 2025.

Furthermore, whilst this review has been framed with a focus on online harms, the Panel is aware that any useful discourse about protection from potential harms has to be balanced with the acknowledgement of the potential benefits that the online and digital world can provide to children and young people. The internet can provide opportunities for learning, connection, creativity, and self-expression, which are all often recognised as beneficial by children and young people. These positive aspects must be considered alongside efforts to mitigate risks and provide safeguards to users.

The purpose of this review has been to highlight an issue that is of significant public interest and act to influence policy and decision makers to take action to ensure that children in Jersey do not have less protection from online harms than their counterparts in other jurisdictions like the U.K.

## Methodology

This report aims to establish what protection is in place for children in Jersey from online harms. The Panel used several methods to gather the evidence that has informed this report and has combined qualitative evidence from stakeholder submissions and public hearings with quantitative data where this is available.

The Panel gathered its primary evidence from public hearings, targeted stakeholder letters and public submissions. Desktop research has been undertaken and a list of reports, academic literature, legislation and policy is referenced in a bibliography at the end of this report.

The majority of the Panel's gathered evidence is qualitative, and this has been analysed thematically to identify recurring concerns and patterns. Furthermore, the review was limited by the availability of Jersey-specific data on online harms and some international comparisons may not fully reflect local context.

The Panel did not engage directly with children or young people during this review, given Scrutiny's non-policy-making role. Nonetheless, the review has made a conscious effort to recognise and incorporate the significance of collecting their perspectives within its findings and recommendations.



## What are online harms and how are they relevant to children in Jersey?

### Defining “online harms”

Broadly, “online harms” refer to any harmful impact or risks that individuals encounter because of digital interactions or use of the internet and online spaces. However, the detail underneath this banner term is wide ranging. There is no definitive internationally recognised definition to encapsulate “online harms”, however, there are various classifications that could help establish a shared understanding of what “online harms” are considered to be, which is particularly important where there are multiple stakeholders and cross-jurisdictional involvement.

The Organisation for Economic Co-operation and Development (‘OECD’) has categorised typology of risks for children in the digital environment in the ‘4C’s’ framework.<sup>1</sup> There are four main risk categories identified, namely:

- **Content** risks (exposure to harmful or inappropriate material);
- **Conduct** risks (risks from a child’s own behaviour online, sharing private personal information);
- **Contact** risks (risks of harmful interactions with others, such as grooming or cyberbullying); and
- **Consumer** risks (sometimes referred to as ‘**contract** risks’, such as scams, or a misuse of personal data).<sup>2</sup>

These are all also impacted by a number of cross-cutting risks:

- **Privacy** risks (interpersonal, institutional and commercial);
- **Advanced technology** risks (e.g. Artificial Intelligence (A.I), Internet of Things (IoT), predictive analytics, biometrics); and
- Risks on **health and wellbeing**.

The United Nations Convention on the Rights of the Child (‘UNCRC’) Committee on the Rights of the Child has published ‘[General Comment No. 25](#)’, which focusses on children’s rights in relation to the digital environment. It provides some examples about what these risks might mean for children in the digital world:

*Risks relating to content, contact, conduct and contract encompass, among other things, violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist.*<sup>3</sup>

Furthermore, the World Economic Forum (‘WEF’) Global Coalition for Digital Safety has outlined six categories of online harms in a “Typology of Online Harms”<sup>4</sup>, which are:

- Threats to personal and community safety;

---

<sup>1</sup> ‘[Children in the Digital Environment: Revised Typology of Risks](#)’, OECD Digital Economy Papers, January 2021, No. 302, p. 7

<sup>2</sup> **Note:** during the factual checking process it was highlighted to the Panel that the NSPCC defines the “consumer / contract” risk as “commerce”.

<sup>3</sup> [General comment No. 25 \(2021\) on children’s rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p. 3

<sup>4</sup> ‘[Toolkit for Digital Safety Design and Interventions and Innovations](#)’: Typology of Online Harms’ Insight Report, World Economic Forum, August 2023



- Harm to health and wellbeing;
- Hate and discrimination;
- Violation of dignity;
- Invasion of privacy; and
- Deception and manipulation.

The aim of the WEF's typology is to provide a common foundational language to facilitate a shared understanding of online safety across jurisdictions and between stakeholders.

In the U.K., online harms, as defined within the context of the Online Safety Act (OSA), refer specifically to **harm experienced by individuals, rather than organisations or businesses**. This definition excludes issues such as data breaches or cybersecurity threats, which fall outside the scope of personal harm.<sup>5</sup>

The Panel's report has included aspects related to data protection, as this is an area that Ministers in Jersey have advised is being worked on to address the risks of online harms in the Island. The Panel has also considered elements of the Government's proposed cybersecurity policy, recognising that while cybersecurity focuses on the protection of infrastructure, systems, networks, devices, and data, it can interlink with online harm caused to individuals (for example, poor cybersecurity could lead to increased exposure to online harms). We do however recognise that different types of online harm require distinct responses and expertise.

Furthermore, it is also important to highlight that, whilst online harms can be caused by illegal activities, for example, child sexual exploitation and abuse or terrorist content, some harms may be caused by activities or behaviour that is legal, for example, exposure to content on the internet that encourages self-harm or suicide.

In considering a definition for "online harms", the Children's Commissioner for Jersey (hereafter the 'Children's Commissioner') also highlighted the important consideration that:

*... what we know to be online harm is not necessarily the same as what children and young people identify as online harm.<sup>6</sup>*

This is important as children's experiences and patterns of internet use are inherently different from adults, therefore relying solely on adult perspectives risks could overlook the unique vulnerabilities and concerns of younger users. The Panel suggests that to accurately capture the nature and impact of online harms, it is essential that the Government of Jersey undertakes dedicated work to understand how children and young people use the internet, and what they consider to be harmful within those spaces.

The Panel has received multiple submissions highlighting concerns around smartphone use and screen time, identifying them as potential sources of harm. While simply having access to a device does not equate to harm, they can act as a direct conduit to digital environments where risks can arise, for example, through exposure to inappropriate content, excessive screen use impacting physical and mental health, or vulnerabilities related to privacy and online interactions.

The Panel recognises that the term "online harms" may be interpreted differently by various stakeholders, and that this broad label could give rise to ambiguity or gaps in understanding.

---

<sup>5</sup> <https://www.gov.uk/guidance/understanding-and-reporting-online-harms-on-your-online-platform> (accessed on 12/08/2025)

<sup>6</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.8

Language is crucial in addressing online harms because it shapes how risks are understood, defined, and tackled across legal, technological, and social domains. Terms like “e-safety,” “online safety,” and “online harms” are often used inconsistently, however, the language is important as it influences public perception, policy development, and cross-border collaboration. When terminology is vague, it can obscure the severity of abuse and dilute accountability.

An example of this is provided by the [Guiding Principles for Addressing Technology-Facilitated Child Sexual Exploitation and Abuse](#) report, which emphasises that without clear, aligned definitions on how technology-facilitated Child Sexual Exploitation and Abuse (‘CSEA’) and related risks might be understood, identified or defined, it can be difficult to appropriately and responsibly deal with or manage associated risks related to technology-facilitated CSEA.<sup>7</sup>

Should the Government of Jersey pursue further initiatives to mitigate risks associated with online harms, we recommend that this work include a clear definition and classification of the specific types of harm being targeted.

This report will refer to different types of harm with the intention of highlighting the variety and scope of potential risks and will set out the measures currently in place to address them.

---

<sup>7</sup> Van der Spuy, Anri et al., [Guiding principles for addressing technology facilitated child sexual exploitation and abuse](#), Digital Futures for Children Centre, December 2024, p.20

Some **examples** of online harm are:



#### FINDING 1



There is currently no internationally recognised definition for “online harms” however, a range of shared classifications and terminology has emerged. Establishing consistent language and definitions is important for improving understanding and addressing the complexities of online harms.



#### RECOMMENDATION 1

The Government of Jersey should ensure that any further work initiatives to address risks related to online harms include clear definitions and classification of the specific types of harm being targeted. This will help to facilitate a shared understanding between different groups of stakeholders and, where applicable, support alignment across jurisdictions.

## Are children and young people considered to be more vulnerable to potential online harms?

Worldwide, there is a growing body of research and evidence being gathered to assess the impact that the online world is having on children's lives. In the U.K. the communications regulator Ofcom shared statistics in April 2025<sup>8</sup> which indicated that:

- 59% of teenage children aged 13-17 reported encountering potentially harmful content online (over a 4-week period);
- 31% of 8–12-year-olds that go online have seen something that they found worrying or nasty;
- 30% of 13–17-year-olds reported encountering online harm from scrolling through their feed or via a 'For You' page;
- Children have said that seeing violent content is "unavoidable"; and
- Of those who have seen online pornography, the average age at which they had first seen it was 13.

Research by the organisation [Internet Matters](#) has identified that "*online harms are not experienced equally*".<sup>9</sup> The Children's Commissioner highlighted the research by Internet Matters to the Panel in a public hearing and shared that the following groups rank among those who are considered most vulnerable online:<sup>10</sup>

- children in care;
- young carers;
- children with special education needs;
- children with communication difficulties;
- children with mental health difficulties; and
- children with physical disabilities.

Internet Matters suggest that it is just as important to understand **who is harmed and how**, in addition to the numbers of children that any online harms issues may affect. There are also indicators from their research that age, gender, and socio-economic background shape the likelihood, type and severity of the risks faced.<sup>11</sup>

In relation to child sexual abuse, the risks related to age and gender were described in the written submission from the Children's Commissioner:

*In a 2023 evidence review the NSPCC highlighted that gender and age remain important factors linked to vulnerability of risk to online sexual risk and harm. For example, girls are found to face every category of online sexual risk more frequently than boys; older adolescents are more likely to report experiences of online sexual abuse. However prepubescent and younger children are more likely to be depicted in child sexual abuse material.*<sup>12</sup>

---

<sup>8</sup> <https://www.ofcom.org.uk/online-safety/protecting-children/new-rules-for-a-safer-generation-of-children-online> (accessed 5<sup>th</sup> August 2025)

<sup>9</sup> <https://www.internetmatters.org/hub/research/rising-harms-new-rules-why-the-online-safety-act-matters/> (accessed 5<sup>th</sup> August 2025)

<sup>10</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.9

<sup>11</sup> <https://www.internetmatters.org/hub/research/rising-harms-new-rules-why-the-online-safety-act-matters/> (accessed 5<sup>th</sup> August 2025)

<sup>12</sup> [Written Submission – Online Harms Review - Children's Commissioner for Jersey](#)

Several written submissions to the Panel also highlighted that online harms are considered a public health issue because of their impact on both mental and physical wellbeing. Former Information Commissioner for Jersey and Guernsey, Emma Martins, opined that the issue of online harms is urgent and said:

*We should be in no doubt that we are in the midst of a public health emergency. Unlike other emergencies, this one is mostly hidden.*<sup>13</sup>

The Panel was provided with a written submission from Public Health Jersey which detailed risks and areas in relation to screen time and children's health:

*The effects of screen use on health and wellbeing are not uniform across all children and young people. Factors such as age, gender, neurodivergence, and socio-economic background can influence the degree and nature of the impact. In Jersey, patterns observed in screen time and wellbeing data suggest that certain groups may be more vulnerable to adverse effects, highlighting the need for targeted and proportionate policy responses.*<sup>14</sup>

The submission names the population groups that could be most impacted by screen use as: girls, neurodivergent children and young people, children living in low-income households and older adolescents.<sup>15</sup>

The Panel also received a written submission from Dr. Chris Edmond, a member of the Health Professionals for Safer Screens group, who shared research from that group on '*The impacts of screen use and social media on whole child health*' which highlighted that the risks of harm to children of Early Years far outweigh any benefits. It detailed developmental issues caused by screen use, physical impacts of screen use, and the societal impact of screen usage.<sup>16</sup>

In relation to privacy and risks to personal data, the Jersey Office of the Information Commissioner advised that "*it is right to acknowledge that rapid technological advancements have increased privacy risks for children and young people in several ways*".<sup>17</sup> In summary, these were identified as:

- **Data collection:** Online platforms, including games and smart toys, often gather large amounts of personal data, sometimes without clear or lawful consent, raising concerns about misuse.
- **Profiling and targeted advertising:** Collected data may be used to profile children, leading to targeted advertising that can shape their choices and behaviour.
- **Lack of understanding:** Children and parents may not fully understand privacy policies or the extent of data shared and collected through online platforms.
- **Exposure to inappropriate content:** Algorithms can expose children to harmful material, and features like direct messaging may put them at risk of contact with deceptive or unsafe users.

This submission also included statistics that 80% of children in the Western world have a digital footprint by age two, and 46% of teenagers are almost constantly online, in part indicating the exposure of younger generations' lives to the digital environment.

Comparisons have frequently been drawn between risks faced by children in the "online world" and those encountered in the "offline world." Ministers emphasised that their focus extended

---

<sup>13</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>14</sup> [Written Submission – Online Harms Review - Public Health Jersey](#)

<sup>15</sup> [Ibid](#)

<sup>16</sup> [Written Submission – Online Harms Review – Dr. Chris Edmond](#)

<sup>17</sup> [Written Submission – Online Harms Review - Jersey Office of the Information Commissioner](#)

beyond online harms to include all risks faced by children wherever they were.<sup>18</sup> The Panel has collected evidence that highlights that there is a recognised interconnection between the online and offline risks, showing that vulnerabilities in digital spaces often mirror or amplify those in offline environments.<sup>19</sup>

An example of this correlation was provided by the Children's Commissioner, who referenced the connection between the online and offline world for bullying:

*...cyberbullying tends to be an extension or a reflection of actual in-person bullying that is also going on. It is not something that frequently happens independently of in-person interaction, so it is a multi-layered issue.*<sup>20</sup>

The Children's Commissioner also referenced 2019 research from [Internet Matters](#) which had found that there was a widening gap between the majority of young people who are digitally adept, and a vulnerable minority whose online life puts them at risk of harm. It was explained that, for vulnerable people, their behaviour in the digital world is influenced by vulnerabilities already present offline and compounded by risks and harms that they encounter online.<sup>21</sup>

It was also highlighted to the Panel that the children who were most vulnerable may be the ones more likely to miss out on online safety education, for example being out of school for medical reasons, or through placement changes if they are in care.<sup>22</sup> This was referred to in a submission to the Panel by one parent who indicated that their vulnerable daughter had been a victim of exploitation as she had reached out to make friends online. The writer questioned: *"What are they now going to do to stop this happening to more vulnerable children that are being let down by education"*.<sup>23</sup>

Furthermore, during the public hearing with the Minister for Children and Families, the Minister said that vulnerable children, including those in care or those with specific needs, might be more likely to be targeted in relation to crimes such as grooming and abuse and he opined that this was where efforts to mitigate those risks needed to be concentrated.<sup>24</sup> As per the Ministerial responsibilities set out in the report 'States of Jersey Law 2005: Article 30A – Ministerial Responsibilities' ([R.118/2024](#)), the Minister for Children and Families has specific responsibility for *"coordinating policies to safeguard children and support children's wellbeing"* therefore the Panel suggests that this Minister should be responsible for Government policy work in this area of online safety.

During the public hearing with the Children's Commissioner, the Panel was informed about the use of *"guardrails"* in relation to A.I., which are defined as protective measures designed to ensure A.I. systems operate safely. It was explained that guardrails can be embedded directly into A.I. technologies but can also be shaped through policy and legislation. The importance of these broader regulatory approaches was particularly emphasised.

---

<sup>18</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#)

<sup>19</sup> Van der Spuy, Anri et al., [Guiding principles for addressing technology facilitated child sexual exploitation and abuse](#), Digital Futures for Children Centre, December 2024, p.32

<sup>20</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.4

<sup>21</sup> [Ibid](#), p.9

<sup>22</sup> [Ibid](#), p.9

<sup>23</sup> [Written Submission – Online Harms Review - Anonymous 18](#)

<sup>24</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.14



It was explained that while technical safeguards are more established, work at the policy and legislative level remains in its early stages. These efforts are often closely tied to data collection and processing practices, which play a central role in how digital platforms engage with users.<sup>25</sup> The Children's Commissioner advised that:

*I would say that I think the important point about A.I. guardrails, however, is that it is not just about the platforms, it is about policy and it is about legislation. You now have organisations, Government organisations, Governments, developing their own ethical policies on A.I. use, and how it is used, what it is used for, what it collects, what it shares. I think that that is something that could, at least in some way, be considered for a whole range of organisations on Jersey that interface with children.<sup>26</sup>*

The Panel believes that the Government of Jersey should actively consider implementing guardrails within policy and legislation as part of its approach to developing A.I. frameworks, with particular emphasis on safeguarding children.

## FINDING 2



Online harms are not experienced equally and in order to address risks it is important to understand *who* is harmed and *how*. Online risks can reflect or intensify the dangers children face offline, with those already vulnerable in real-world settings more likely to be at risk in digital spaces.

## FINDING 3



Protective measures or “guardrails” can be used in policy and legislation development in relation to technology developments, such as artificial intelligence and other emerging digital tools. These safeguards help ensure that innovation is balanced with ethical considerations, user safety, and the protection of fundamental rights, particularly for vulnerable groups such as children and young people.

## RECOMMENDATION 2



The Minister for Children and Families should coordinate work to assess the risks and impact of different online harms to all children and identify vulnerable groups in order to develop targeted interventions. This work would inform policy decisions and ensure that safeguarding measures are inclusive, evidence based and responsive to emerging threats.



## RECOMMENDATION 3

The Government of Jersey should explore the development of policy and legislative guardrails to ensure the safe, ethical, and responsible use of artificial intelligence across public and private sectors. The guardrails should be designed for all users but consider special protections for children.

<sup>25</sup> [Letter – Online Harms Review - Follow up from Children's Commissioner – 30<sup>th</sup> July 2025](#)

<sup>26</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.19



## Impact of online harms on children in Jersey

In a written submission to the Panel, former Information Commissioner for Jersey and Guernsey, Emma Martins, succinctly summarised the challenge of protecting children in Jersey from online harms:

*Living and parenting in Jersey has always offered a largely safe and beautiful environment. But the digital world knows no geographical boundaries and our children and young people are exposed to, and at risk from, the same harms as every other 'connected' person across the globe.<sup>27</sup>*

When evaluating the impact of online harm on children in Jersey, the Panel was faced with the limitations of local data to assess the specific effects of online harm, however, we have collated a few statistics and examples for this section.

Although the Panel did not conduct its own formal survey or consultation as part of this review, we invited submissions from members of the public to capture a sense of public sentiment (all public submissions can be accessed on the Panel's review page, [here](#)). Most responses concerning online harm focused on screen time and smartphone usage. While the terms of reference for the review did not focus on these areas, it is evident that screens and smartphones are widely perceived as gateways to forms of online harm. Whilst personal accounts can offer valuable insight into children's online experiences, they are not sufficient for determining the scale or prevalence of online harm.

In a public hearing the Panel asked the Children's Commissioner what children and young people had shared with her office about their digital lives, and whether online harms had any impact. It was stated that adults were more likely to raise issues related to online harms (like use of smartphones or managing social media), rather than the subject being raised by children themselves:

*When we went out to consultation last April for our strategic priorities, digital safety or online harms did not emerge from children as an issue that they thought we should be focusing on. It did, however, emerge from adults who raised several issues around cyber bullying, around protection from the online world, about managing social media, but they were raised predominantly by adults, not by children themselves.<sup>28</sup>*

The Panel asked if the Children's Commissioner was surprised that online safety had not been raised as an issue, but she explained that "My previous work with children would suggest that this is not something that a lot of children specifically see as being dangerous to them".<sup>29</sup> This approach was also reflected in a response provided by the Minister for Children and Families who had expressed surprise that he had not been asked any questions about online safety during a visit to a school and had been advised by the teacher that children already had a very good understanding of what they should be looking for and the issues on the internet.<sup>30</sup>

It is interesting to consider whether there is a disconnect between adult assumptions about online risks and children's own perceptions of danger and it potentially highlights the importance of grounding policy and educational initiatives in children's lived experiences and perspectives. This is explored further in the section '[What action can Jersey take to provide children with a safer digital future?](#)'.

---

<sup>27</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>28</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.3

<sup>29</sup> [Ibid](#), p.4

<sup>30</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.7

The Panel contacted the Minister for Justice and Home Affairs to request data from the States of Jersey Police concerning recorded reports and offences involving online crimes against children, such as online harassment, grooming, or threatening behaviour via telecommunications. In response, the Minister shared the requested data with the Panel on a confidential basis, explaining that due to the low number of cases in certain categories, there was a risk of identifying individual victims. However, during the course of the review, the Panel had noted a Jersey court case which identified that over 40 children had been targeted by a drug syndicate through social media. The Panel was interested to understand what Jersey could learn from cases like this. The Children's Commissioner advised that:

*I think the principal lesson for us from that is that Jersey is not immune from this kind of exploitation. We absolutely cannot be complacent but that this activity happens in the Island and our children will be targeted. There will be attempts at exploitation and we need to be extremely aware of that.*<sup>31</sup>

The Panel notes that, although this case is not necessarily indicative of a broader trend, it nonetheless highlights that **serious exploitation can occur locally through online and digital channels**. This underscores the need for Government attention and intervention.

Nevertheless, the criminal cases and States of Jersey Police data represents only a partial, tip of the iceberg view, as it does not currently account for online harm concerns which are not criminal activity, such as a child viewing inappropriate content or engaging in potentially harmful, addictive behaviours related to online gaming or excessive device use. This demonstrates the scale of online harms and importance of definitions.

In May 2022 the Government of Jersey published a report: '[Children and the Digital World](#)', which found that there was "*a high level of self-awareness amongst the children and young people (10-18 years) who acknowledged that they spent 'too much' time online and used words such as addiction and anxiety when referring to their use of devices and / or specific applications along with a drive for this to change*".<sup>32</sup>

This report had collected data in 2021, following the impact of the Covid-19 pandemic in 2020. The unknown impact of the pandemic was referenced by the Children's Commissioner who explained that even 4-5 years after the pandemic event, it was difficult to fully understand the impact it has had on children's digital lives. With reference to the reversal of the world moving online during the pandemic, she stated that "*I simply think we do not even yet know what or how the reversal and the expected reversal of that for children has actually affected them*".<sup>33</sup>

The Panel asked Ministers about the key learnings derived from the [Children and the Digital World](#) report and if any subsequent initiatives had been undertaken in response. The Minister for Children and Families confirmed that the report had provided key insights, including "*the need for consistent digital education, stronger family-focused guidance, and early support around the emotional and psychological effects of online harms, including screen time, cyberbullying, and digital addiction*".<sup>34</sup> He explained that the key responses included:

- the launch of the Digital Education Strategy;
- a review of online safety systems across schools and children's care homes; and
- that a review of the CYPES online safety policy and Digital Harm Guidance is underway.

---

<sup>31</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.10

<sup>32</sup> [Children and the Digital World](#), Government of Jersey, May 2022, p.5

<sup>33</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.10

<sup>34</sup> [Letter – Online Harms Review – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

However, the Minister also provided some criticism of the report, highlighting that whilst it recognised lots of the digital developments following the Covid-19 pandemic were positive, he opined that:

*I do not think it recognised the danger is twofold, obviously the safeguarding, but also the amount of time spent on devices.<sup>35</sup>*

The [Jersey Children and Young People's Survey](#) (JCYPS) has locally collected and published data about "e-safety" and other factors like the use of social media. In 2024 the survey found that:

- 63% of Year 6 children owned a smartphone, rising to 100% in Year 12;
- 37% of young people (years 6, 8, 10 and 12) had sent messages to a stranger online, with a higher proportion of females (40%) doing this, compared to males (34%);
- 93% of females and 88% of males in Year 12 (typically 16-17 years old) had one or more social media accounts in their own name;
- 20% of male pupils and 14% of female pupils in Year 4 (typically 8-9 years old) and 30% of male pupils and 25% of female pupils in Year 6 (typically 10-11 years old) had social media accounts in their own name;
- 20% of males and 19% of females had lied to their parents and carers about who they speak to online;
- 22% of all respondents had changed or removed the privacy settings on social media sites to attract more friends and followers; and
- 28% of young people reported receiving a sexual photo or video online (a decrease from 36% in 2021).<sup>36</sup>

These statistics were discussed in a public hearing that the Panel had with the Children's Commissioner:

*I think that is something that we should be concerned about. When you combine that [numbers indicating social media accounts in own name] with the figures from the survey that show the proportion of all children who have lied or misled their parents in relation to their online activity, who are bypassing all the safety provisions on social media websites and also have talked to strangers via these websites, I think that presents a worrying picture for children, for parents, for Government and for society at large it should present a worrying picture.<sup>37</sup>*

When the JCYPS data was discussed with the Minister for Children and Families it was referenced that some of the statistics were lower in the 2024 survey than they had been in the previous survey (in 2021), for example, in response to the question "Have you ever received a sexual video or photo?". In 2021 36% of all year 8s, Year 10s and Year 12s responded "yes", but this had fallen to 27% of these same age groups in 2024.<sup>38</sup> The Minister explained that he thought that it was important to question whether this was "a real drop" or if data is skewed.

In a submission to the Panel from Public Health Jersey, which focussed on screen time and children's health, it was advised that the data collected by the JCYPS indicated that Jersey was following global trends. The statistics quoted were:

- 39% of students spent over five hours on screens the previous day;

---

<sup>35</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.40

<sup>36</sup> [Jersey Children and Young People's Survey Report 2024](#), Statistics Jersey, 26<sup>th</sup> March 2025

<sup>37</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.6 (square brackets added for context)

<sup>38</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.32

- Fewer than half the respondents slept for eight hours;
- 22% of respondents met daily activity guidelines, dropping to 8% among older girls;
- Higher anxiety reported in females; and
- 22% of older students reporting thoughts of self-harm.<sup>39</sup>

The submission highlights that causality cannot be assumed, but that **the patterns indicated the need to further explore and understand screen use and its health impacts in order to shape effective policy in Jersey.**<sup>40</sup>

The topics outlined in this section offer a glimpse into the wide-ranging nature of online harms. In the sections that follow, we will delve deeper into identifying who is affected and in what ways, while also examining the existing safeguards and proposed strategies aimed at protecting children from various forms of online harm.

#### **FINDING 4: Key Finding**



Although Jersey has been typically regarded as a safe environment for children, it remains vulnerable to the risks associated with the online world. The borderless nature of digital spaces means that children and young people in the Island can be exposed to harmful content and influences originating from anywhere in the world. A recent court ruling has brought to light a case involving the exploitation of local children where communications have been facilitated by online platforms.

#### **FINDING 5**



Digital safety or online harms is not an issue that has been raised as a worry or concern by children themselves with the Children's Commissioner for Jersey, or the Minister for Children and Families. Instead, issues affecting children's health and safety online are more often voiced by parents and other adults.

#### **FINDING 6: Key Finding**



Issues around smartphone and screen use have been highlighted to the Panel by members of the public and through locally collected data. Public Health has referenced data in the Jersey Children and Young People's Survey and has suggested that emerging patterns warrant deeper investigation to better understand the health impacts of screen use and inform policy development in Jersey.

<sup>39</sup> [Written Submission – Online Harms Review – Public Health Jersey](#)

<sup>40</sup> [Ibid](#)

## Legacy of the Independent Jersey Care Inquiry

For Jersey, one of the most significant contextual aspects is the legacy of the 2017 Independent Jersey Care Inquiry (hereafter, the 'Inquiry'), which made significant recommendations about how Jersey should transform its child-care system after decades of failings.

The Government of Jersey has taken action to address the Inquiry's recommendations, however, there are enduring aspects that can be taken from the recommendations and the lessons learnt.

At an operational level, one of the responses to the Inquiry was the implementation of the '[Jersey's Children First](#)' practice framework. This is used by various agencies and is designed to both improve and coordinate the work of practitioners working with children and families. A submission to the Panel by a mental health practitioner advocated for regulatory measures that reinforce the framework, stating: "*Please see a way to proposing meaningful, robust regulation that supports the Jersey's Children First approach, and supports our families, and the next generation*".<sup>41</sup>

The Panel is of the opinion that there needs to be continued consideration of the Inquiry's recommendations and lessons in order to effectively learn from the past, and so it is relevant to raise this as a factor in the way that Jersey has addressed the risk of online harms to date, and plans to address it in the future.

Recommendation 5 of the Inquiry highlighted that legislation had lagged behind other jurisdictions in the developed world. Whilst this specific recommendation referenced legislation related to child-care and youth justice, the Panel is concerned that there could be parallels with addressing children's welfare with regards to online safety.

The Inquiry also set out "*eight basic lessons to be learned from the failures of the past*"<sup>42</sup> which included:

***The welfare and interests of children are paramount and trump all other considerations. Traditional values, operating and management practices, the needs or employment status of staff, convenience, HR practices and the reputation of the island should all be secondary considerations to the interests and welfare of children.***<sup>43</sup>

The Panel queried Ministers about this as a principle and was assured by the Minister for Children and Families that it was a priority consideration:

***Deputy H.M. Miles:***

*Because part of the lessons learned from the care inquiry included that the welfare and interests of children are paramount and trump all other considerations. As the Minister with responsibility for children, do you believe that that principle is being properly applied to our modern challenges?*

***The Minister for Children and Families:***

---

<sup>41</sup> [Written Submission – Online Harms Review – Anonymous 15](#)

<sup>42</sup> The Report of the Independent Jersey Care Inquiry 2017, [Volume 1: Executive Summary](#), 3<sup>rd</sup> July 2017, p.54

<sup>43</sup> Ibid, p.55

*I think that is the case. I do not think there are any States Members or departments that believe that this is something that can be left and not dealt with. I think any matters regarding children have to be given priority, so that is absolutely paramount.*<sup>44</sup>

The Panel asked the Minister for Sustainable Economic Development if an assessment of children's rights or a Child Rights Impact Assessment (CRIA) was undertaken as part of the analysis of the option of a permissive extent clause for Jersey in the U.K.'s OSA, as part of the decision-making process in relation whether Jersey should request a permissive extent clause be included in the U.K.'s OSA. It was confirmed that this had not been done.<sup>45</sup> The Panel was concerned to learn this, as one of the main objectives of the OSA was to make internet services safer for individuals and impose certain duties that required providers to ensure that services provided a higher standard of protection for children than for adults.<sup>46</sup>

Under the [Children \(Convention Rights\) \(Jersey\) Law 2022](#), all propositions submitted to the States Assembly must be accompanied by a CRIA. This assessment serves to evaluate how the proposal may affect children and whether it aligns with the relevant articles of the UNCRC. Whilst the CRIA is only required at the point of lodging it is good practice and would fulfil its intended purpose to conduct it at the early stage in the policy consideration and development process.

#### **FINDING 7: Key Finding**



No assessment of children's rights was undertaken as part of the analysis of the option of a permissive extent clause for Jersey in the U.K.'s Online Safety Act, despite the legislation's purpose to improve online safety for children. The Panel is concerned that this demonstrates that the lessons and recommendations from the Independent Jersey Care Inquiry (for example, ensuring that the interests of children are paramount and that legislation does not lag behind other jurisdictions) are not widely embedded into practice across the whole of Government.



#### **RECOMMENDATION 4: Key Recommendation**

Policy considerations should be subject to a formal assessment of children's rights at an early stage. The Government of Jersey should evidence how it will embed this process across all departments to reflect the enduring lessons of the Independent Jersey Care Inquiry.

<sup>44</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.22

<sup>45</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.9

<sup>46</sup> Online Safety Act 2023, <https://www.legislation.gov.uk/ukpga/2023/50> (accessed 19th August 2025)



## What are children's rights in the digital environment?

The United Nations Convention on the Rights of the Child (UNCRC) is an international treaty, first adopted by the United Nations in 1989, which sets out civil, political, economic, social, and cultural rights of every child. It was ratified by Jersey in 2014.

With regards to children's rights in the digital environment the Children's Commissioner's written submission to the Panel said that *"a balanced approach is required – one that maximises the benefits of the digital world whilst ensuring children's protection and safety"* and further explained that *"when designed and used appropriately, digital technology can advance children's rights and well-being"*.<sup>47</sup> Some of the relevant UNCRC Articles highlighted to the Panel by the Children's Commissioner for Jersey<sup>48</sup> are:



<sup>47</sup> [Written Submission – Children's Commissioner for Jersey](#)

<sup>48</sup> Ibid



The Panel was also advised by the Children's Commissioner that in addition to the UNCRC, certain Articles of the European Convention on Human Rights (ECHR) were particularly relevant<sup>49</sup>:

- **Article 8 (Right to Respect for Private and Family Life):** This applies to children's digital rights, such as their right to privacy in digital communications and online activities. This includes protecting children from breaches of privacy, online harassment, and unauthorised use of their personal data.
- **Article 10 (Freedom of Expression):** This article grants children the right to access and share information online, but it must be balanced against protections against harmful content, such as online hate speech or abusive materials.
- **Article 14 (Prohibition of Discrimination):** This article applies to children's protection from online discrimination, such as cyberbullying based on gender, race, or other factors.

In 2021 the UNCRC's Committee on the Rights of the Child (the 'Committee') published its [General Comment No. 25](#) (2021) on children's rights in relation to the digital environment, which outlines how states can support rights in this context and confirms that the UNCRC rights apply equally to the digital environment as the non-digital world. It outlines four principles as a lens to view children's rights in relation to the digital environment:

- Non-discrimination;
- Best interests of the child;
- Right to life, survival and development; and
- Respect for views of the child.

The Panel has also noted commentary about Article 3 of the UNCRC in relation to the digital environment. Article 3 refers to the 'best interests of the child' and a report compiled as research for the [Digital Futures for Children Centre](#) has stated that there is evidence of misunderstanding this phrase of "best interests" in relation to the digital environment, suggesting that in some contexts it is being used as a substitute for a full range of children's rights which could, amongst other things, legitimise a "*one-size-fits-all*" approach that does not consider children's diverse circumstances.<sup>50</sup> The report emphasises the importance of a full spectrum of children's rights, without putting some ahead of others, highlighting that rights are interlinked and that trading rights could be disadvantageous to the child. Furthermore, the report explains that "*determining the best interests of children should not be confused with the task of balancing children's interests against the desires of parents or the commercial interests of companies*".<sup>51</sup>

In her public submission to the Panel, Victoria O'Neil cited the UNCRC commentary acknowledging the potential of digital technology to enhance children's rights but emphasised the importance of striking a balance between upholding children's rights in the digital sphere and fulfilling the duty to protect them from potential online risks. She suggested that this was not being realised in practice and that ensuring safety and protection should take precedence:

*A child learning how to code through Computer Science or using spreadsheets with Information Technology and enhancing their digital literacy is what I believe the UNCRC are referring to. But I would argue in the case of online harms, most are*

---

<sup>49</sup> [Written Submission – Online Harms Review - Children's Commissioner for Jersey](#)

<sup>50</sup> Sonia Livingstone et al., [The Best Interests of the Child in the Digital Environment](#), Digital Futures for Children Centre, March 2024, p. 2

<sup>51</sup> Ibid, p. 1

*proliferated via a smartphone which is not referred to by the Children's Commissioner. A smart phone gives easy access to social media platforms like Snapchat or TikTok, and I would argue that a delay to this would not be an infringement of their rights and would protect them until they are able to make responsible choices for themselves.<sup>52</sup>*

In response to queries from the Panel about how the Government reviewed its compliance with the UNCRC, the Minister for Children and Families shared the importance of Article 19 (i.e. protection from harm). He expanded the response to explain how policies to address exploitation of children were monitored through the Children, Young People and Families' Plan 2024-2027 (the 'CYPF Plan') and the Children's Outcomes Executive Committee:

***The Minister for Children and Families:***

*So our Children and Young People (Jersey) Law 2022 has set out senior officer and ministerial responsibilities for safeguarding children and that is in line with general comment number 25. So in effect the legal arrangements in that law do not distinguish between online and offline harms, but the responsibilities are the same. We have multiagency safeguarding policies on children exploitation. How we monitor those, again it comes to the Children's Outcomes Executive Committee, which oversees our Children, Young People and Families' Plan. Within that we have material that is in line with the UNCRC, and in fact each of the sections within the plan has the relevant areas of the UNCRC highlighted and how they tie back to it.<sup>53</sup>*

The Panel asked the Children's Commissioner about how the Government should be assessing its obligations under the UNCRC. The Children's Commissioner outlined that the Government needed to have a good understanding of their duties under each of the UNCRC articles, taking advice from the relevant general comments where possible. She explained that:

*I think one of the best tools that the Government has available to it at the moment, and should absolutely be applied in this context, is the Child Rights Impact Assessment tools. I think they are essential for looking at digital policies, I think they are essential for looking at digital platforms and services, and they can promote and prioritise the safety and well-being of children.<sup>54</sup>*

As previously highlighted, the Panel observes that presenting the CRIA only at the point of lodging a proposition may limit its influence on shaping policy.

**FINDING 8**



The United Nations Convention on the Rights of the Child (UNCRC) Rights are equally applicable to children in the digital environment, and all rights must be considered equally. In practice, a tailored approach is essential and there is no one-size-fits-all solution to a rights approach, as all children's circumstances will be different.

<sup>52</sup> [Written Submission – Online Harms Review - Victoria O'Neil](#)

<sup>53</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.30

<sup>54</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.15

## Why did Jersey reject the option of a permissive extent clause to the U.K.'s Online Safety Act?

The Panel was concerned that as a result of declining the option of a permissive extent clause for the OSA, internet users in Jersey, particularly children, would have an increased risk of being exposed to online harms due to potential gaps in legislation between jurisdictions. The Panel set out to try and understand what those gaps, if any, might be and what the Government had done to analyse this in advance of the decision.

### What is a permissive extent clause?

A permissive extent clause (PEC) is a legal mechanism that allows certain provisions of a U.K. Act of Parliament to be extended to the Crown Dependencies or Overseas Territories, with agreement from the relevant jurisdiction.

Article 31 of the [States of Jersey 2005](#) sets out the procedures relevant to the question of U.K. legislation extending to Jersey:

#### **31 Duty to refer certain matters to the States**

- (1) Where it is proposed –
  - (a) that any provision of a draft Act of the Parliament of the United Kingdom should apply directly to Jersey; or
  - (b) that an Order in Council should be made extending to Jersey –
    - (i) any provision of an Act of the Parliament of the United Kingdom, or
    - (ii) any Measure, pursuant to the Channel Islands (Church Legislation) Measures 1931 and 1957,the Chief Minister shall lodge the proposal in order that the States may signify their views on it.
- (2) Where, upon transmission of an Act of the Parliament of the United Kingdom containing a provision described in paragraph (1) (a) or of an Order in Council described in paragraph (1)(b) to the Royal Court for registration, it appears to the Royal Court that the States have not signified their agreement to the substance of the provision or Order in Council –
  - (a) the Royal Court shall refer the provision or Order in Council to the Chief Minister; and
  - (b) the Chief Minister shall, in accordance with paragraph (1), refer it to the States.

In summary, Article 31 sets out the requirement that the Government of Jersey seek approval from the States Assembly before requesting that a U.K. Act of Parliament be extended to Jersey via an Order in Council, i.e. it is used where the Government has agreed to extend a U.K. Act, or certain provisions of a U.K. Act, to Jersey and the negotiations for

PECs are used in areas where it is felt necessary to coordinate laws between the U.K. and Crown Dependencies, for example, matters relating to nationality and borders, national security, fisheries and radio broadcasting.

The decision to include a PEC in a draft U.K. Act does not involve a formal process that is prescribed by law. The Panel's understanding is that early discussions take place between the Jersey Government and U.K. Government and, following any period of research and negotiations, the final decision to consent or reject the inclusion of a PEC in a draft U.K. Act rests with the Minister, or Ministers, in Jersey with political responsibility for the policy subject area. The purpose of the Article 31 clause is to ensure that Jersey's sovereignty is maintained and that the U.K. cannot impose legislation on the Island.

Furthermore, we understand that it would be a political matter as to whether the Minister would look to raise at Council of Ministers the question of a PEC being included in a U.K. Act before giving their response to the U.K. Department.

### How was the decision about the OSA PEC made?

In respect to the consideration of the draft OSA the following response was provided to a written question ([W.Q.144/2024](#)) in the States Assembly:

*The Minister for Sustainable Economic Development made the decision in September 2022 not to pursue a Permissive Extent Clause in the Online Safety Act. This followed a review of the UK legislation and corresponding Jersey law which indicated that Jersey could legislate locally for the same purposes (if desired). Officers in Economy and Justice and Home Affairs are scoping legislation to protect against digital harms, alongside incorporating recommendations from the Violence Against Women and Girls Task Force.*<sup>55</sup>

In the public hearing on 4<sup>th</sup> October 2024 the Minister for Sustainable Economic Development advised that he was asked to make a decision about the permissive extent clause to the draft OSA in November 2022. He explained that:

*The draft law at that point, which is what I was asked to decide upon, had been carefully examined by officers and an analysis had been undertaken on that and presented to me. As a result of that analysis, I felt that a permissive extent clause would not have been appropriate for Jersey for a number of reasons.*<sup>56</sup>

The Minister also opined that jurisdictions other than the U.K. might provide better examples of better routes for Jersey to take:

*I do not believe the U.K. has set off on the right path on this, or the best path. We can look at other places; Australia I know is coming out very strongly as a law which looks really quite good. Possibly the Irish one does as well. We can look at them and model our own law based on what they are doing, rather than just taking what the U.K. did. It moved really fast, the U.K., on this law, but it did not necessarily ... by seeking speed, it may not have got the quality that it needs.*<sup>57</sup>

The Minister set out the reasons that the option of a PEC had been declined, which included that:

- the OSA was a “poor law”<sup>58</sup> and Jersey could learn from the U.K.’s mistakes and take a more focused and proportionate approach;
- Jersey should preserve its autonomy and create its own law, or laws, “because we can and should legislate for ourselves”<sup>59</sup>;
- Where a law was brought to Jersey through a permissive extent clause, there would be no way for Jersey to amend it in the future; and

---

<sup>55</sup> [W.Q.144/2024](#) (To the Minister for Children and Families, by Deputy C.D. Curtis, April 2024)

<sup>56</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.6

<sup>57</sup> [Ibid](#), p.17

<sup>58</sup> [Ibid](#), p.6

<sup>59</sup> [Ibid](#), p.7

- the OSA was “over-complexified”<sup>60</sup>, it would be hard for Ofcom to enforce and would not fit the needs for Jersey and its smaller population.

The Minister said that by not adopting the OSA, Jersey would have the opportunity to develop its own bespoke legislation. He explained that:

*Then we will have a law in Jersey, or several laws in Jersey, aiming to protect Islanders from inappropriate and dangerous content on the internet and we will be able to change that, make sure it keeps up with technology long into the future. That is what the States of Jersey is for. The States of Jersey is not there just to take what the U.K. creates and bring it into our books where we have no ability to change it in the future.*<sup>61</sup>

The Panel asked for details about the research and analysis that was presented to the Minister in order for him to make this decision. In a letter sent on 17<sup>th</sup> March 2025, the Panel asked: *Please can you provide the Panel with a copy of the analysis you received in November 2022 (and any other relevant documentation) which was used to inform your decision to reject the permissive extent of the UK’s Online Safety Act for Jersey.* The Panel was not provided with any copy of analysis documentation and the written response from the Minister for Sustainable Economic Development on 21<sup>st</sup> March 2025 was:

*We strongly believe that as a self-governing dependency of the Crown, it is imperative that Jersey remains responsible for its own legal and regulatory frameworks and that the States Assembly develops, debates and provides oversight of legislation whenever it is able to do so. This ensure that legislation is proportionate and right-sized for Jersey and can be amended by the States Assembly.*<sup>62</sup>

The Panel wanted to understand how much of the decision to reject the PEC was made on a principle of Jersey legislating for itself and the weighting of the other evidence contributing to the decision, including consideration of children’s rights. During the public hearing on 16<sup>th</sup> May 2025 the Minister for Sustainable Economic Development advised that the point of principle was a factor in the decision:

**Deputy C.D. Curtis:**

*What consultation or discussion did you have with other Ministers in Government about making this decision?*

**The Minister for Sustainable Economic Development:**

*I did not, I was asked to make this decision on my own.*

**Deputy C.D. Curtis:**

*Would there not normally be a discussion with other Ministers around something that might affect the welfare of children?*

**The Minister for Sustainable Economic Development:**

*It was not suggested to me at the time and because I felt that Jersey ... and it is a point of principle. Jersey is here to legislate for itself. We are not here just to take the U.K.’s laws and put them on our books. From my perspective, the important thing was that*

---

<sup>60</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.8

<sup>61</sup> [Ibid](#), p.6-7

<sup>62</sup> [Letter – Online Harms Review – Minister for Sustainable Economic Development – 31<sup>st</sup> March 2025](#)



*Jersey works to legislate on this, and I spoke to the then Minister for Home Affairs, Deputy Miles, and made it very clear at the time that we would be very happy to work with this and make sure we get the laws on to Jersey's books as appropriate, but laws which are proportionate.*<sup>63</sup>

Later in the same hearing the Panel questioned this further. The Minister advised that the point of principle was not the sole factor in the decision, and it was largely related to the perceived problems with the OSA:

***The Connétable of Grouville:***

*[...] You have already advised the panel about your reasons behind the decision not to pursue the permissive extent clause for the Online Safety Act. However, can you confirm if this decision was made on principle or did any research and analysis back up that decision?*

***The Minister for Sustainable Economic Development:***

*So, no, it was not made solely on principle at all. It was made as well because of what I would say were clear and glaring problems with the Online Safety Act, one of them I have mentioned already in this hearing, was this idea of something legal but harmful which was creating, just through a single Act in the U.K. Government, a new concept in law, which had not been discussed, had not been decided or proven. It famously runs for over 300 pages, the U.K. Online Safety Act. It was clear to me that it was overly complex, it required enormous bureaucracy, and so in itself I still believe, and I will come to the point where I believe I have been shown to be correct in my thinking, is it was always in my view going to be an unworkable law that would effectively be ineffective but would make the Government of the time feel good that it was doing something to supposedly protect children, to protect people, tick a box. It is a 300-page tick box exercise. So deeply unproportionate for Jersey. But there are, from a general permissive extent clause perspective, any law that Jersey brings into its own body of law via a permissive extent clause is by definition a law that the States of Jersey cannot amend.*<sup>64</sup>

The Violence Against Women and Girls Taskforce report gave an account of Jersey's decision not to pursue a PEC within the OSA, indicating that it was partly based on principle and influenced by the experience of previous negotiations between Jersey and the U.K. on other matters:

*The UK Department that holds responsibility for the Online Safety Bill - Digital, Culture, Media and Sport (DCMS) - contacted the Government of Jersey to seek clarification of our position regarding the extension of certain provisions of the Online Safety Bill to Jersey. However, the UK Government's recognition of the importance of gaining the consent of crown dependencies before extending UK legislation has fluctuated in recent years, as was well publicised in 2018 and 2019 in relation to issues with regard to the extension of UK fishing legislation. As a result, Ministers directed officers to request that no permissive extent clauses for Jersey be included within the UK Online Safety Bill. Whilst the Taskforce recognises the importance of preserving Jersey's*

---

<sup>63</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.8

<sup>64</sup> [Ibid](#), p.24



*autonomy, and that an extension of the Bill may not be desirable or appropriate, we do have concerns around the regulation of online platforms, such as Facebook and Instagram, on the island. Without an extension of the Bill to Jersey, Ofcom has no ability to regulate these platforms or hold them accountable if they fail to protect islanders from harmful content. Moreover, there is currently no alternative regulatory body that would have the power to do so in Jersey.*<sup>65</sup>

The Panel notes that there was no formal Ministerial decision to formally record the consideration of the PEC offer (thereby it did not come to the attention of Scrutiny), and the Panel was advised that it was recorded in minutes and an officer's report at the time.<sup>66</sup>

The Minister for Sustainable Economic Development advised that, at the time he had consulted with the Minister for Home Affairs but not the Minister for Children and Families.<sup>67</sup> Individuals in the Ministerial positions have changed since the time of the decision in 2022, however, the current Minister for Children and Families confirmed that he was supportive of the approach taken by the Minister for Sustainable Economic Development:

*There is actually quite a bit of criticism about the U.K. online law that has recently been introduced, in that it really started looking at inappropriate content and then spread out into a number of other areas. The belief is that it has become so complex that it is difficult to enforce in some cases. I think we need to avoid that. I am wholly supportive - and you will hear from the Minister for Sustainable Economic Development - of a local law. This is a fast-changing world, and legislation has to be able to keep up to it. If we had been part of U.K. legislation, it would be impossible to change it without going to the U.K. first. So I am wholly supportive of a local law.*<sup>68</sup>

During a later public hearing with the Minister for Children and Families on 23<sup>rd</sup> May 2025 the Minister repeated his criticism of the U.K. approach and legislation and also suggested that the NSPCC had been critical of the OSA. However, the Panel contacted the NSPCC after the hearing and it was clarified that some of the comments made by the Minister did not accurately reflect the NSPCC's position, their response to this can be accessed [here](#).

The Minister for Sustainable Economic Development advised the Panel that the decision not to accept the PEC to the OSA was not informed by any impact assessment to consider child rights.<sup>69</sup> As previously outlined, the Panel was concerned to learn that a CRIA had not been undertaken as part of the decision-making process.<sup>70</sup>

The Panel asked the Children's Commissioner for Jersey if she was aware whether there was any consultation with her office (prior to the current Commissioner's appointment) on this matter and it was advised that there was not:

---

<sup>65</sup> [‘The issue of violence against women and girls in Jersey’](#), a report by the Taskforce on Violence Against Women and Girls, November 2023, p. 91

<sup>66</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.9

<sup>67</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.8

<sup>68</sup> [Ibid](#), p.5

<sup>69</sup> [Ibid](#), p.9

<sup>70</sup> [Ibid](#), p.9

**Deputy H.M. Miles:**

*I know you said that that predates you, but do you know whether the Office of the Children's Commissioner was consulted as part of that review?*

**The Children's Commissioner:**

*To the best of my knowledge, no, we were not consulted.*

**Deputy H.M. Miles:**

*Would you expect to be consulted?*

**The Children's Commissioner:**

*Yes, I think this is an issue that is core to children's rights and therefore, yes, we would expect to be consulted.<sup>71</sup>*

In the same public hearing, the Children's Commissioner advised the Panel that it was important to understand the basis of the Government's decision in relation to the PEC and the assessment that had been undertaken with regards to legislative protections:

*I believe at the time that the Government was considering whether or not to agree to the P.E.C., they undertook a review of the Jersey Legal Framework against what was the proposed Online Safety Bill. I personally would be interested to understand exactly what that review found, because I think it is important that we really understand and know the basis for the decision for not taking the P.E.C. Also, what the level of online protections for children in Jersey that the Government felt were already in existence and what the options were considered in terms of addressing any gaps in that. There is mention since then by various Ministers of ... and it is on the public record, by the development of bespoke legislation, but personally for us it remains unclear as to what the scope or nature of what that legislation would cover.<sup>72</sup>*

The Panel was interested to understand whether the decision in 2022 not to adopt the PEC initiated the work on alternative legislation based on the assessment that took place ahead of the decision in late 2022. In October 2024 the Minister for Sustainable Economic Development advised that:

*We are absolutely working on the legislation both through the Telecommunications Law and the Data Protection Law. I know that the Minister for Justice and Home Affairs is working on the Sexual Offences Law.<sup>73</sup>*

The Panel found out that the most progressed work in relation to legislation to provide protection against online harms was in relation to the recommendations from the Violence Against Women and Girls (VAWG) Taskforce report. However, as the Taskforce's report was not published until 9th November 2023, the Panel suggests that it cannot be said that these

---

<sup>71</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.13

<sup>72</sup> [Ibid](#), p.12-13

<sup>73</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p. 13

legislative developments were directly driven by the rejection of the PEC, consideration of any respective legislative gaps, and a desire to explore alternative solutions at that time in 2022.

In a hearing with the Information Commissioner the Panel asked whether Jersey's government should have adopted the U.K. Online Safety Act via the PEC, and whether doing so would have made the Information Commissioner's work easier. The Commissioner responded to say that it might have assisted in some areas but highlighted that the scope is outside of their current remit, so clarified that it would be hard to assess. He emphasised the need for ensuring that any legislation was future-proofed and suggested that a principles-based approach would offer better long-term resilience.<sup>74</sup>

### How will Jersey internet users be classified?

As referred to in the introduction one of the principal drivers for this review was interest from the Panel to understand if, or how, Jersey internet users would be impacted by the introduction of the OSA in the U.K.

In a hearing on 4<sup>th</sup> October 2024 the Panel questioned whether Jersey's decision not to adopt the U.K.'s OSA or the E.U.'s DSA could result in Jersey users being treated as "rest of the world" by websites, potentially leading to different user experiences, for example in relation to age restrictions. The Minister for Sustainable Economic Development admitted uncertainty about the risk but suggested that Jersey could mitigate it by aligning its laws with the principles of U.K. and E.U. legislation, as it has done with data protection laws post-Brexit. He confirmed that question would be explored by the Government during the course of its work.<sup>75</sup>

The Panel followed this up at the public hearing with the same Minister on 16<sup>th</sup> May 2025. It was explained that it was difficult to establish a complete picture of this matter, but Ministers referenced expectations of an "umbrella effect" from the OSA:

#### ***The Connétable of Grouville:***

*Very well indeed, so we thank you. During the public hearing on 4th October 2024, the panel asked a question regarding potential risk of Jersey users being classified within a "rest of the world" category when accessing certain websites and, at the time, that was not known. Could you confirm whether any efforts have been made to assess that or establish a position on that?*

#### ***Senior Policy Officer, Department for the Economy:***

*Yes, it is very hard to establish the total picture because each internet provider and each online platform manages their world classification in slightly different ways. A total picture is very hard to get. Also how people in Jersey access those platforms is many and varied, so some people have a U.K. SIM card but will be accessing it via Jersey internet providers when they are on wi-fi, for instance, but by U.K. providers when they are on 4 or 5G so it is a very hard question to quantify.*

#### ***The Minister for Sustainable Economic Development:***

---

<sup>74</sup> [Transcript – Online Harms Review Public Hearing – Jersey Office of the Information Commissioner – 7<sup>th</sup> July 2025](#), p. 18

<sup>75</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.28-29

*Due to the umbrella effect that I was talking about earlier, certainly I hear the experience of most Islanders at the moment is we continue to fall under the U.K. classification for most providers of any content.<sup>76</sup>*

This understanding was shared by the Assistant Minister:

***Assistant Minister for Sustainable Economic Development:***

*I can only speculate, but if the U.K. is going to do this anyway, what value does it really add? They are going to do it, they are going to be saying to internet providers: "You must do this", and this affects everybody.<sup>77</sup>*

During the hearing the Minister for Sustainable Economic Development explained that Jersey would benefit indirectly from U.K. content-blocking laws due to shared infrastructure (such as dialling codes) but that it would also introduce its own legislation tailored to local needs which would draw best practice from around the world. He said:

***The Minister for Sustainable Economic Development:***

*We will benefit from it to some extent anyway indirectly and just by the provision, because again, because Jersey will fall under the effectively the dialling code for the U.K., then anything that is prohibited in the U.K., through U.K. law, will not reach Jersey either, just because we are in effectively the same part of the system as they are. But, on top of that, we are then going to have our own Law, so we are going to have an indirect benefit from that, or anything the U.K. does, not to remove content, but to block content, to block access. All of that is going to happen to Jersey just because the umbrella of it. But then we are going to have our own Law separate to that which will be of direct benefit to Islanders and will be amendable by the States of Jersey, so we will be able to respond to new technologies. I think really importantly is what we are doing, the U.K. may have been first, but the U.K. are first and worst in this case, I am afraid, and we have the benefit of looking at other jurisdictions and how they are dealing with this. We are looking at using them, we are looking at Australia, we are looking at European nations as well and how they are dealing with it, and not just blindly following the U.K. down what, in this case, is a blind alley.<sup>78</sup>*

In the same hearing the Minister also advised the Panel that:

***The Minister for Sustainable Economic Development:***

*Again, I have to say that with Europe and U.K. - and I bring Europe into that on purpose as well because I know they look down these routes as well - we are going to be caught under the umbrella. I think the reality is that, if the U.K. brings in age verification for pornography or any sites, anyone in Jersey wanting to access them is probably going to have to engage with that U.K. age verification system of where we sit today. That is the truth of it.<sup>79</sup>*

---

<sup>76</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.27

<sup>77</sup> [Ibid](#), p.26

<sup>78</sup> [Ibid](#), p.26

<sup>79</sup> [Ibid](#), p.28

On 25<sup>th</sup> July 2025 the child safety provisions of the OSA legislation came into force in the U.K. which required, amongst other things, robust age-verification procedures to be put in place on sites with adult content. As an example, websites which have publicly announced that they will be taking these steps include Porn Hub, Blusky, Discord, Grindr, Reddit and X.<sup>80</sup>

The Panel had concluded its evidence gathering by the commencement date on 25<sup>th</sup> July 2025, however, members of the Panel attempted to test the age verification required for accessing certain adult websites. It was found that only a click box to confirm age was required.

Whilst this was not an official assessment, we believe that this shows that the comments the Minister for Sustainable Economic Development made about the “*umbrella effect*” was not correct in relation to age verification requirements on certain websites. Panel officers subsequently made informal email inquiries to websites directly and, from those that responded, we learned that because Jersey is not subject to the U.K.’s Online Safety Act, they have therefore not implemented age-assurance in line with the OSA for users in Jersey.

The Panel acknowledges that individual companies and digital platforms may adopt varying approaches to implementing age-assurance measures. However, it emphasises the underlying **concern that children in Jersey may now face fewer barriers, compared to their counterparts in the U.K., when attempting to access content that is not considered age appropriate**. If Jersey continues to depend on U.K. based internet safety advice and guidance, given that the regulatory parameters have now clearly diverged any gaps need to be identified.

The Panel is concerned about Ministerial claims regarding the “*umbrella effect*” of the OSA for Jersey users, particularly in areas such as age verification, given the lack of clear evidence to substantiate this position.

### Alignment with other jurisdictions, including the Crown Dependencies

During the course of the review that Panel learned that the other Crown Dependencies, Guernsey and the Isle of Man, had accepted the inclusion of a PEC in the OSA.<sup>81</sup> The Panel understands that neither of the jurisdictions have currently activated their PEC, however, were they to do so Jersey would be in a standalone position.

The Panel has set out the evidence collected from the Minister for Sustainable Economic Development about his reasons for deciding not to accept the PEC and that domestic legislation was the best route forward.

The Panel received a number of opinions from the public about whether or not Jersey should align itself with the U.K.’s OSA. One submission suggested that “*any attempt to ‘go it alone’ in this space risks being **symbolic rather than effective***”<sup>82</sup> and it went on to highlight the case for extending U.K. legislation to Jersey:

*Whilst it does not square with Jersey as a distinct jurisdiction, we must if legislation is to have any chance of altering the behaviour of online platforms act in concert with other (larger jurisdictions).*

---

<sup>80</sup> [Online age checks now in force - Ofcom](#) (accessed 1<sup>st</sup> August 2025)

<sup>81</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.25

<sup>82</sup> [Written Submission – Online Harms Review – Anonymous 19](#)

*Rather than developing a bespoke framework, I would recommend that Jersey should adopt/extend UK measures, such as the Online Safety Act, to ensure alignment with a larger, more influential regulatory regime. This would:*

- *Provide consistency for platforms operating in both jurisdictions.*
- *Leverage the UK's enforcement infrastructure and regulatory expertise.*
- *Ensure Jersey residents benefit from the same protections as those in the UK.*<sup>83</sup>

Other submissions the Panel received were opposed and “*urged the States of Jersey to maintain independence from this legislation*”<sup>84</sup> due to concerns about it having a negative impact on freedom of expression, privacy and censorship.

### PEC process summary

This report will remain silent on whether Jersey should or should not have requested the inclusion of a PEC in the U.K.'s OSA, however, **the Panel is critical of the process by which that decision was made and is unconvinced that the decision was made with adequate consideration of all relevant factors particularly with regard to the fact that a central aim of the U.K.'s Online Safety Act is to ensure that children receive a higher level of protection from potential harms associated with internet services.**

Looking to the future, the Panel is concerned that different rules across jurisdictions could cause confusion in an area that needs global cooperation. Working in line with other countries would help create a clear and effective system, especially for maintaining consistent oversight standards.

#### FINDING 9



There is a requirement for the States Assembly to approve the extension of any U.K. Act to Jersey, however, there is no formal process or requirement for permissive extent clauses which are offered for Jersey to be discussed by the States Assembly or Council of Ministers, and the decision making power as to whether to reject them lies with the Minister who is deemed to have political responsibility for the relevant area in question. To ensure greater transparency, future decisions should involve clearer information sharing with both the Council of Ministers and Scrutiny.

#### FINDING 10



The decision not to request a permissive extent clause for Jersey in the U.K.'s Online Safety Act was made solely by the Minister for Sustainable Economic Development during the period September – November 2022. The reasoning given for this was that the U.K.'s Online Safety Act was considered to be an overly complex “poor” law, a “tick-box exercise” and, because of the principle that Jersey should legislate for itself.

#### FINDING 11



The Minister for Sustainable Economic Development's decision was not recorded in a formal Ministerial decision or shared with the Council of Ministers so there was no opportunity for scrutiny and no transparent decision-making process.

<sup>83</sup> [Written Submission – Online Harms Review – Anonymous 19](#)

<sup>84</sup> [Written Submission – Online Harms Review - Cardin Pasturel](#)



#### FINDING 12



The Minister for Sustainable Economic Development did not consult the Office of the Children's Commissioner, or the Minister with responsibility for coordinating policies relating to children despite the fact that a central aim of the U.K.'s Online Safety Act is to ensure that children receive a higher level of protection from potential harms associated with internet services.

#### FINDING 13



There is no evidence that the Minister for Sustainable Economic Development's decision to reject the permissive extent clause for the U.K.'s Online Safety Act in late 2022, initiated any alternative work to assess how local legislation could be developed to provide alternative protection for users in Jersey.

#### FINDING 14: Key Finding



In May 2025, the Minister for Sustainable Economic Development informed the Panel that regulatory changes in the U.K. and Europe might create an "*umbrella effect*" for Jersey users. Specifically, if the U.K. introduced age verification for certain websites, Jersey users would likely need to comply with the U.K.'s system. However, when the Panel informally tested this assumption in July 2025, after the U.K.'s child safety provisions took effect, it was found that Jersey was not covered by the age verification changes. Therefore, children in Jersey may now face fewer barriers, compared to their counterparts in the U.K., when attempting to access content that is not considered age appropriate.

#### FINDING 15



Jersey is a potential anomaly compared to the other Crown Dependencies of Guernsey and the Isle of Man, which both opted to request a permissive extent clause be included the U.K.'s Online Safety Act, however, the Panel was advised in May 2025 that neither of the other Crown Dependencies had 'activated' its permissive extent clause.

#### RECOMMENDATION 5



The Government of Jersey should create a formal process which widens the scrutiny available to the option of a permissive extent clause prior to the decision being made. As a minimum a Ministerial decision should be required, so that the relevant Scrutiny Panel and members of the States Assembly and general public have the opportunity to raise questions.

#### RECOMMENDATION 6



The Government of Jersey should formally research and assess what "*umbrella effect*", if any, there is for Jersey internet users from the U.K.'s Online Safety Act and the E.U.'s Digital Services Act. Assessment findings should be published for public transparency.

## **How are children in Jersey currently protected from types of online harm?**

As part of the review's terms of reference (see Appendix 1) the Panel sought to examine and establish the protection in place for children with consideration of:

- Legislation and regulations;
- Government Policy;
- Role of Internet Service providers and technology;
- The role of social media platforms, content providers and content creators; and
- The role of education, family and culture.

Reflecting on the aspects outlined above, there is an inevitable overlap between the questions explored in this section and the next: namely, 'how are children protected?' and 'who is responsible for protecting children from online harms?' To minimise repetition, this section focussing on the 'how', will provide a high-level overview of the current legislative and policy landscape, followed by subsections that examine specific forms of online harm, in order to provide insight into the protections currently in place.

The subsequent section will shift focus to the 'who,' outlining the ideal roles and responsibilities of parents, educators, and other stakeholders within a 'safety-by-design' framework and identifying how they do this.

### **Legislation**

Some of the main themes of the Panel's queries to Ministers were about whether legislation should form part of the protections that are put in place for children from online harms, what work had been done to assess existing legislation before the permissive extent clause was rejected, and what planned legislative changes or updates, if any, were being developed.

This section outlines the protections currently afforded by existing legislation, as well as the jurisdictional and enforcement challenges associated with regulating issues such as online harm. Details shared with the Panel regarding proposed or potential legislative developments will be explored in greater depth later in the report (in the section headed '[What action can Jersey take to provide children with a safer digital future?](#)').

At a public hearing on 23<sup>rd</sup> May 2025, the Minister for Children and Families stated that there were protections from online harms in place from existing laws in Jersey:

*Some of our existing laws already are a good basis for protection; they are already providing a level of protection, even though they were not designed for this specific purpose. They are protecting children as well as adults, and I think retaining that flexibility by enhancing existing legislation, which should be relatively quicker than a complete new suite of legislation, I would say that is the way forward.<sup>85</sup>*

On the following pages the Panel has set out a table which attempts to provide a high-level explanation of the legislation currently in place and, where relevant, legislation planned for the future. **This should not be taken as a comprehensive list or considered as legal advice:**

---

<sup>85</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.7

| Type of harm                                                                                                                   | Current Legislation                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Creation of, or exposure to, child sexual abuse material (CSAM) (for example, indecent images of children)                     | Sexual Offences (Jersey) Law 2018<br><br>Protection of Children (Jersey) Law 1994<br><br>Telecommunications (Jersey) Law 2002 (Article 51)                                                                                                                                                                                                                                                                                                                   |
| Exposure to other inappropriate or unsuitable content, such as pornography, violent content, terrorist content, or hate speech | Telecommunications (Jersey) Law 2002 (Article 51) may be relevant in some instances                                                                                                                                                                                                                                                                                                                                                                          |
| Inciting or promoting self-harm or suicide                                                                                     | Homicide (Jersey) Law 1986                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Online grooming                                                                                                                | Sexual Offences (Jersey) Law 2018<br>[ <b>Note:</b> Further legislation is in development that can be used to prosecute online grooming activity that involves intimate image abuse or cyberstalking as a result of VAWG]                                                                                                                                                                                                                                    |
| Harassment                                                                                                                     | The Crime (Public Order) (Jersey) Law 2024<br>[ <b>Note:</b> the harassment offence cannot be applied to conduct that occurs on only one occasion, e.g. one-off communications sent on social media]<br>Further legislation is in development as a result of VAWG                                                                                                                                                                                            |
| Stalking                                                                                                                       | None<br><br>[ <b>Note:</b> Further legislation is in development as a result of VAWG]                                                                                                                                                                                                                                                                                                                                                                        |
| Cyberbullying                                                                                                                  | Telecommunications (Jersey) Law 2002 (Article 51)                                                                                                                                                                                                                                                                                                                                                                                                            |
| Fraud and scams                                                                                                                | Fraud is a customary offence in Jersey, and the elements of the offence have been set out in the case <i>Foster – v – Attorney General</i> 1992                                                                                                                                                                                                                                                                                                              |
| Sale of illegal goods                                                                                                          | Potentially covered by fraud (particularly if there is a misrepresentation as to the status or legality of the goods)<br>Consumer protection is provided under the Supply of Goods and Services (Jersey) Law 2009 and the Distance Selling (Jersey) Law 2007 (which particularly governs the sale of goods or services at a distance and applies to sales carried out via the internet, text messaging or by telephone)<br>Misuse of Drugs (Jersey) Law 1978 |
| Privacy violations (including identity theft, data misuse, data profiling, etc)                                                | The Protection of Children (Jersey) Law 1994<br><br>Data Protection (Jersey) Law 2018<br><br>[ <b>Note:</b> Cybersecurity Law is in development]                                                                                                                                                                                                                                                                                                             |
| “Misinformation” and “Disinformation” (i.e. “fake news”)                                                                       | None                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                                         |                                                                                                                        |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Preventing sale of addictive substances to minors       | Not related to online harms, but there are laws which prohibit the sale of alcohol and tobacco to minors <sup>86</sup> |
| Potential negative impact on mental and physical health | None                                                                                                                   |

In addition to the above, the Panel is aware of the following legislation, which would be relevant in certain circumstances:

- [Sex Offenders \(Jersey\) Law 2010](#) - also offers a measure of protection against repeat offending by allowing the Courts to order that people convicted of relevant offences may have their online access restricted or monitored for as long as necessary to protect the public.
- [Computer Misuse \(Jersey\) Law 1995](#) – The purpose of the law is to make provision for securing computer material against unauthorised access or modification and for connected purposes. (This was highlighted as relevant legislation to the Panel by the Minister for Children and Families in the public hearing on [23<sup>rd</sup> May 2025](#)).
- [Cybercrime \(Jersey\) Law 2019](#) – strengthens provisions for evidence gathering retention of evidence and international cooperation in investigating crimes.
- [Children \(Jersey\) Law 2002](#) – the legislation which consolidates the law relating to children.
- [Children and Young People \(Jersey\) Law 2022](#) – the purpose of this law is to make provision to promote and support the wellbeing, and safeguard the welfare, of children and young people. This does not name particular types of harm, but it does define “corporate parents” and provide “responsible Ministers” and “safeguarding partners” with responsibilities for safeguarding for children and young people. The Panel was advised that the law does not discriminate around online and offline, and that it applies to both.<sup>87</sup>

The Panel has heard that Article 51 of the [Telecommunications \(Jersey\) Law 2002](#) is one of the most relevant areas of existing legislation that can be used to protect children from potential online harms. This legislation was updated in 2016 (via the [Telecommunications \(Amendment No. 3\) and Crime \(Miscellaneous Provisions\) \(Jersey\) Law 2016](#) in P.19/2016). Key changes at that time included amending the Telecommunications (Jersey) Law 2002 to expand the definition of offences to cover improper use of any telecommunications system, not just public networks. Offences include sending grossly offensive, indecent, obscene, or menacing messages, knowingly or recklessly, as well as sending false messages or persistent misuse intended to cause distress. Penalties were increased to up to 2 years’ imprisonment and an unlimited fine.

It is worth noting that P.19/2016 also made amendments to the Crime (Disorderly Conduct and Harassment) (Jersey) Law 2008. Courts were empowered to issue restraining orders upon conviction for any offence, not just harassment, if necessary to protect victims from further harm or threats. Penalties for harassment and breach of restraining orders were also raised to match those in the updated Telecommunications Law.

<sup>86</sup> Namely [‘Restriction on Smoking \(Cigarettes to Children\) \(Jersey\) Regulations 1992](#) and [Licencing \(Jersey\) Law 1974](#)

<sup>87</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.11

The Panel asked the Minister for Sustainable Economic Development if Article 51 of the telecommunications law was considered to be robust enough for a lot of the digital and the online offences, for example around A.I. The Minister responded to say:

*Enforcement, really it creates an offence, so I regard that very much as within the remit of the Minister for Justice and Home Affairs. So I cannot report how many people complained about these things because, as you can see, the onus is put on the individual that is using the system rather than the telecoms provider themselves for which it is more within the remit of our department.<sup>88</sup>*

With legislation there are jurisdictional challenges with enforcing the law, as any potential defendant would need to be within, or to be brought within, the geographical jurisdiction of Jersey's courts.

In the public hearing held on 4 October 2024, the Minister for Children and Families said that he was “*wholly supportive*” of local legislation to ensure online safety for children, rather than aligning with or adopting the OSA:

**Deputy C.D. Curtis:**

*[...] Does ensuring online safety for children, as you are the Minister for Children and Families, do you think that that requires a legislative approach from Government?*

**The Minister for Children and Families:**

*Legislation is useful as a tool. Would it make any difference today if the legislation was there? I do not think it would change our approach. I think that our approach is extremely good, despite the fact that legislation is not here. When it gets there, it is a tool that might allow us to request certain content to be blocked.<sup>89</sup>*

One of the aspects of the decision not to request a PEC for Jersey was the principle that Jersey should legislate for itself (see above section “[Why did Jersey reject the option of a permissive extent clause to the U.K.'s Online Safety Act?](#)”). However, the potential risk and “*futility of a small jurisdiction acting alone*”<sup>90</sup> on this issue has been highlighted and is a major concern for the Panel, with regards to the challenges of enforcing any local legislation outside of the Island and compliance from digital platforms which operate internationally. A number of written submissions to the review reference this point:

*Without the scale or influence to enforce compliance, Jersey-specific regulations may be ignored or circumvented by major platforms. Worse, they may create **duplicative or inconsistent obligations** that complicate enforcement and dilute the impact of broader efforts.*

*Additionally, where online platforms are located in the USA, their “home” legal and regulatory environment may be significantly less strict, meaning that unless we are going to start blocking websites (a possibility but probably no more than that), the scope for regulation is probably limited.<sup>91</sup>*

---

<sup>88</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.17

<sup>89</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.5

<sup>90</sup> [Written Submission – Online Harms Review – Anonymous 19](#)

<sup>91</sup> [Written Submission – Online Harms Review – Anonymous 19](#)

Former Information Commissioner for Jersey and Guernsey, Emma Martins, advised the Panel that:

*We are not a large jurisdiction. That means we have to face the reality of what enforcement outside of our borders looks like. It also means we can be nimble, and we can be responsive, but that requires us to be proactive, deliberate and thoughtful and to unite in a common aim.*

*Jersey also prides itself on its independence and this is an opportunity for us to be clear about what we want (and don't want) for our children and young people and to put that into action. In this, our children are not, as they are in so many other areas of their lives, protected from harms beyond our borders.<sup>92</sup>*

The above submission also highlights that unlike other areas that are influenced by physical borders, the internet operates without such constraints, thereby altering the conventional characteristics typically associated with an island jurisdiction.

In a discussion about drafting new legislation, the Panel heard about the importance of language focussing on the harm itself and to be neutral about the means of that harm:

**Associate Director of Criminal Justice Policy:**

*[...] part of the art, we are coming to suspect, is not to chase tech, simply state your harms, make it abundantly clear, so for instance the stalking piece, to be neutral about whether or not it is happening in the street or online. So, if you arrange it right, you can be stalked in person, you can be stalked by telephone, you can be stalked over the internet, you should be able to be stalked by brain implant. The harm is concentrated on, if the legislation is neutral about the tech, it should last, it should have a long enough lifespan that it will capture stuff as you go forward. It is where novel things emerge, it is where technology takes you to a place where new types of things are happening. That is when the law, I find, tends to be left behind, honestly.<sup>93</sup>*

This neutral approach would ensure that the law would remain relevant and adaptable for any future unknown developments, and there is a risk that if legislation is too tied to particular technologies, it could become outdated and inefficient.

Whilst we will address the potential legislative change later in this report, the work that the Government is doing in response to the Violence Against Women and Girls Taskforce report (hereafter the 'VAWG report') warrants acknowledgement in this section.

In response to queries from the Panel about the work Government is doing to protect children from online harms, Ministers have cited upcoming legislative reforms being prepared in response to the VAWG report, which was published in November 2023. In recommendation 10 of the VAWG report, the Taskforce urged the Government of Jersey to introduce comparable safeguards to those provided under the U.K.'s OSA, particularly in relation to the regulation of online platforms and their responsibility to protect users, through alternative legislative mechanisms. The report further noted that the Taskforce had received advice suggesting that alignment with the European Commission's DSA could serve as a suitable substitute for the OSA.

---

<sup>92</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>93</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.16



In relation to the proposed legislation, the Children's Commissioner said:

*For me what is less clear is how the intended protections for platform users, including children, that have been introduced under the U.K. Online Safety Act, such as the requirement on platforms to prevent children from accessing harmful material, age inappropriate content, to provide clear and really accessible ways to report, which I think is critically important, are actually going to be addressed in Jersey.<sup>94</sup>*

The Panel has attempted to gather some information about this and, where possible, will set out details in the sections on '[Types of Online Harm](#)' in a later section of this report.

#### **FINDING 16**



Ministers advised that existing legislation in Jersey may offer some protection against online harms. However, the scope of this legislation appears to be disjointed, addressing only certain types of harm and lacking comprehensive coverage of the full range of risks children and young people face in the digital environment.

#### **FINDING 17**



Ministers have indicated that further legislation could be developed to enhance protections against online harms. However, concerns remain regarding the practical challenges of enforcement, particularly given Jersey's position as a small jurisdiction. The Panel also noted the complexities of legislating independently on an issue that is inherently international in nature, where influence over global digital platforms may be limited.

#### **FINDING 18**



The Violence Against Women and Girls (VAWG) legislation currently in development offers an opportunity to address online harms. However, its scope does not specifically focus on children, which potentially leaves a gap in protections for young people in the digital environment.

#### **FINDING 19**



The Panel was advised that any legislation aimed at providing protection should focus on the harm itself rather than the technology through which it occurs. A technology neutral approach ensures laws remain effective as new digital threats emerge, while technology-specific laws risk becoming outdated.

#### **RECOMMENDATION 7: Key Recommendation**



The Government of Jersey should conduct and publish a comprehensive gap analysis of existing legislation addressing online harms, with particular attention to the range of types of harm currently covered. This analysis should also consider the absence of child-specific protections in emerging frameworks such as the VAWG legislation and reflect the enforcement challenges faced by a small jurisdiction operating in a global digital environment.

<sup>94</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.12

## Policy

Multiple policy areas intersect in ways that could contribute to enhancing protections against online harms. The Panel was interested in determining whether, and how different policy areas intersected in the protection from online harms.

The Minister for Children and Families explained that Jersey's compliance with the UNCRC is embedded within its legal and policy frameworks. He highlighted that the *Children and Young People (Jersey) Law 2022* establishes clear responsibilities for safeguarding children, aligning with the UNCRC's General Comment No. 25, which affirms that children's rights apply fully in the digital environment. The Minister said that the law treats online and offline harms equally and that:

*We have multiagency safeguarding policies on children exploitation. How we monitor those, again it comes to the Children's Outcomes Executive Committee, which oversees our Children, Young People and Families' Plan.*<sup>95</sup>

Currently, overarching across Government is the CYPF Plan') (published by the Minister for Children and Families). The CYPF Plan is a strategic plan which is required by the Children and Young People (Jersey) Law 2022 and sets out what the Government "*want to achieve for children and young people and should enable better collective decision making about services and facilities*".<sup>96</sup> The plan explicitly references relevant UNCRC articles throughout, ensuring that policy actions are tied back to the UNCRC.

It was confirmed that the CYPF Plan uses survey data to assess trends through an outcomes-based accountability framework, which was monitored by the Children's Outcomes Executive Committee.<sup>97</sup> However, the Panel noted that the CYPF Plan has very limited references to online safety and digital life and questioned this in writing to the Minister for Children and Families. The Minister responded to say that the big picture outcome to ensure that "*all children in Jersey are safe and loved*"<sup>98</sup> was relevant. The Panel queried what progress there was on data collection from the indicators in the CYPF Plan, for example the percentage of young people who feel safe online. The Minister advised that, as part of the data development agenda the CYPF Plan proposed including an indicator to capture "*% of young people (aged 12-18) who feel safe (at school, at home, at work, online, in the community, where they live)*" however, this indicator "*remains under review*".<sup>99</sup>

With regards to updates to operational policy, in the public hearing with the Minister for Children and Families, the Assistant Director of Policy advised that:

*[...] there has been a lot of work done by safeguarding leads to bring forward arrangements and look at operational policy that is keeping up with and reflects some of the harms on those online platforms. That work is ongoing and you can see from the submission from*

---

<sup>95</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.30

<sup>96</sup> '[Children, Young People and Families' Plan for 2024-2027](#)', Government of Jersey, May 2024, p.3

<sup>97</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.20

<sup>98</sup> [Letter – Minister for Children and Families to CEHA Panel following public hearing – 9<sup>th</sup> June 2025](#)

<sup>99</sup> [Ibid](#)

*the safeguarding partnership and N.S.P.C.C. some of the joint work that is ongoing. I think that might be helpful for the panel to hear that.*<sup>100</sup>

In the [written submission](#) to the Panel from the Safeguarding Partnership Business Team,<sup>101</sup> they indicate that the Safeguarding Partnership and the NSPCC held a joint conference in November 2024 focussing on safeguarding children in the digital world. This brought together more than 250 professionals from 98 services across the Government of Jersey, private and charitable sectors. The purpose of the conference was to raise public awareness about Child Sexual Abuse and Exploitation (CSAE), the [CSAE strategy](#), and to highlight lived experiences and encourage island-wide action.<sup>102</sup>

As part of this review, the Panel has heard about the Digital Economy Programme and was advised that:

*In the digital space, the 2025 Business Plan for the Department for the Economy includes the intention to explore options to provide Islanders with the necessary legislation to remove unlawful or intimidating content from online spaces; the implementation of a proportionate telecoms security framework for Jersey and the development and delivery of the draft Cyber Security (Jersey) Law.*<sup>103</sup>

The Panel asked the Minister and Assistant Minister for Sustainable Economic Development if the Department for the Economy had made contact with the Safeguarding Partnership Board about the work they were doing on online harms. During the public hearing the Assistant Minister advised that there had been no specific contact and explained that this was the work that they were doing was not specifically for children, but it would include benefits for children.<sup>104</sup>

The Panel asked the Minister for Justice and Home Affairs to describe how, or if, the protection of children from online harms is considered within, or coordinated into, any policy work she was responsible for, namely 'Justice policy' and 'Criminal justice and community safety policy'. The Minister responded to say that "*the Building a Safer Community Framework provides the framework under which coordination would take place in this area however specific policy work in this area has to date been provided by the Safeguarding Partnership Board*".<sup>105</sup>

In a public hearing the Panel asked how the Building a Safer Community (BASC) Framework, which had been updated and published in 2024, would be part of future policy work relating to the protection of children from online harms. It was explained that the BASC framework was a whole system approach to community safety, but work was ongoing to assess both the overlap and differences between community safety responsibilities and safeguarding. In relation to BASC, the Chief Officer for Justice and Home Affairs explained:

---

<sup>100</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.11

<sup>101</sup> **Note:** During the factual checking process, it was clarified that the Safeguarding Partnership Board was disbanded at the end of 2024 following the introduction of the Children and Young People (Jersey) Law 2022. The responsibility for safeguarding rests with the Safeguarding Partners, as defined by that law.

<sup>102</sup> [Written Submission – Online Harms Review – The Safeguarding Partnership Board](#)

<sup>103</sup> [Letter – Minister for Sustainable Economic Development – 31<sup>st</sup> March 2025](#)

<sup>104</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.35-36

<sup>105</sup> [Letter – Minister for Justice and Home Affairs – 10<sup>th</sup> March 2025](#)

*So for me that has got an absolute link to the online safety, but we are just building really what it looks like from a framework and governance point of view. Now really it is about what we can do and how we can do it, but you do need some structure around it. So I would say it is a work in progress. B.A.S.C. absolutely has a place here as an umbrella, and we want people pulling together and all heading in the same direction and not duplicating.*<sup>106</sup>

The Department for Children, Young People, Education and Skills (CYPES) has produced the Digital Education Strategy and various Safeguarding policies (published on gov.je, [here](#)) including the current Online Safety Policy and the [Jersey Keeping Children Safe in Education policy](#), which are examined in more detail below in the ‘[During school time](#)’ section.

The Panel learned that the Government had established a cross-Ministerial group in September/October 2024 which had been created as a forum to discuss online harms and would continue to meet quarterly.<sup>107</sup> The group consisted of four Ministers, namely the Minister for Children and Families, Minister for Education and Lifelong Learning, Minister for Justice and Home Affairs, and the Minister for Sustainable Economic Development. Despite forming in 2024, during public hearings in May 2025 it became clear to the Panel that the cross-Ministerial group had not formally appointed a Chair to lead its work. The Minister for Justice and Home Affairs advised that a Chair had not been appointed<sup>108</sup>, the Minister for Sustainable Economic Development indicated that there was a “*roving chair*”<sup>109</sup> and the Minister for Children and Families indicated that on the occasion of the Panel’s previous meeting it had been the Assistant Minister for Sustainable Economic Development.<sup>110</sup> The Panel was also advised that Terms of Reference for the Group had not been prepared, but that “*the initial piece of work was about mapping all of the different connections in terms of the legislative programme and connecting the key Ministers and officers together*”.<sup>111</sup>

The Panel also learned in May 2025 that there was a proposal to establish a cross-departmental officer group to support the ministerial group. The Chief Officer for Justice and Home Affairs advised that “*Putting an officer structure in place, it would be slightly wider as well than the Ministers that are already involved. So Public Health, for example, are very interested in this, and there is obviously real concerns and impact there.*”<sup>112</sup>

## FINDING 20



Various Government policies play a role in addressing elements of online safety and providing protection from online harm but there is not an established interconnection between them. It has been suggested that the Building a Safer Community framework could be used to coordinate work.

<sup>106</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.19

<sup>107</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.34

<sup>108</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.10

<sup>109</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.35

<sup>110</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.17

<sup>111</sup> [Ibid](#), p.29

<sup>112</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.11



#### FINDING 21

The Department for the Economy has not had any collaboration with the Safeguarding Partnership Board in relation to their work about online harms, as its work had not been focussed on children.



#### FINDING 22

A cross-Ministerial group was created in September / October 2024 to consider the Government of Jersey's approach to protection against online harms, however, no Chair had been appointed as of May 2025. The Panel also learned that an officer group would be established to support this work.



#### RECOMMENDATION 8

The Government of Jersey should review its procedures to ensure that all Government departments are taking consideration of the impact of their work on children, as an automatic and integrated part of the policy development process.



#### RECOMMENDATION 9

The cross-Ministerial group should publish its terms of reference and provide details to scrutiny about the work it is doing to align relevant policies, data collection efforts, and governance frameworks to demonstrate that there is a coordinated approach to strategic planning and effective oversight to safeguard children and young people from online harms.

## Internet Service Providers

An Internet Service Provider ('ISP') is company or organisation that offers access to the internet through technologies like broadband or wireless.

In the U.K. the [Digital Economy Act 2017](#) introduced a legal requirement for ISPs to implement a filtering service that blocks access to certain content, for example websites that infringe copyright, extremist content, adult content that does not require age verification, and sites that host child sexual abuse material. However, due to the evolution of the digital landscape and challenges with the original age-verification regulator, there were considered to be limitations in the U.K. law, which is why the OSA was introduced to address broader scope of harmful content, such as cyberbullying and promotion of suicide and self-harm.

The Panel was interested to understand whether ISPs played any role in filtering content in Jersey. In a submission to the Panel from one local ISP, JT, they highlighted that Jersey does not have an equivalent law to the U.K.'s Digital Economy Act:

*Jersey does not have a similar legislation mirroring the UK legislation and therefore ISPs do not have a legal basis on which to carry out any blocking or filtering. This puts ISPs in a difficult position, while morally we feel it is right to protect citizens, especially those that are considered vulnerable such as children, without legislation and specific guidelines and procedures in place, JT cannot make the decision on what should or should not be blocked.<sup>113</sup>*

The submission went on to highlight that JT does not implement network-level filtering or blocking across its ISP infrastructure. The company's ability to restrict access is limited to domain name system (DNS) server-level blocking, which prevents users relying on JT's DNS from accessing certain websites, however, users can easily circumvent these blocks by

<sup>113</sup> [Written Submission – Online Harms Review - JT – 4<sup>th</sup> April 2025](#)



switching to alternative DNS providers, such as Google Public DNS (8.8.8.8 / 8.8.4.4). Therefore, it does not prevent access to content for users who are technically proficient or privacy conscious.<sup>114</sup>

In a public submission to the Panel, Jon Tarrant, highlighted that “*There is a significant shortfall in the online protection that is afforded to children in Jersey due to the lack of voluntary measures and formal regulation of Internet Service Providers*”.<sup>115</sup> His submission goes on to query why Ministers have not required Jersey’s ISPs to offer network level protection to users and highlights that:

*The risks of online harm exist for all children regardless of where or when they happen to be online: Jersey’s children are no exception. It is lamentable that the UK introduced these measures more than a decade ago yet there has been no visible progress in this direction in Jersey throughout that period.*<sup>116</sup>

His submission further suggests:

*In the absence of voluntary (opt-in) measures, the Government of Jersey should require all on-Island ISPs to introduce network-level filtering that is active by default and customisable by the contract holder (over 18s). The timescale for the implementation of network-level filtering should be specific and brief, having been achieved in the UK within an 18-month deadline.*<sup>117</sup>

As part of this review, the Panel has not examined the reasons why Jersey did not develop an equivalent to the U.K.’s Digital Economy Act 2017. However, it considers that targeted filtering of illegal online content may be a reasonable option to explore in order to enhance protection for all citizens, particularly children, from harmful material. Given the likely level of public interest in this issue, any future proposals should include a public consultation, with specific efforts to engage children and young people as a matter of course.

A factor highlighted to the Panel as part of the review is the increasing use of Virtual Private Networks (VPNs), which are used by individuals to bypass DNS based restrictions and enhance privacy, rendering basic blocking methods ineffective. JT explained that while more robust content filtering systems exist, implementing them would require significant investment in infrastructure and technology.<sup>118</sup>

This creates a potential challenge for any legislation that is implemented in a jurisdiction relating to online and digital services, as it means that any user can circumnavigate restrictions by using a VPN from another country. The Minister for Sustainable Economic Development advised the Panel that:

*To be honest, anything jurisdictional around the internet full stop becomes a problem because of virtual private networks [...] ... and proxy I.P. [internet protocol] addresses, because you can basically pretend you are somewhere else in the world.*<sup>119</sup>

---

<sup>114</sup> [Ibid](#)

<sup>115</sup> [Written Submission – Online Harms Review – Jon Tarrant – 23<sup>rd</sup> May 2025](#)

<sup>116</sup> [Ibid](#)

<sup>117</sup> [Ibid](#)

<sup>118</sup> [Written Submission – Online Harms Review - JT – 4<sup>th</sup> April 2025](#)

<sup>119</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.18-19



The Head of the Digital Forensics Unit at the States of Jersey Police noted that VPNs, once requiring technical expertise to configure, are now widely accessible as consumer services:

*A few years back, you would need to have technological abilities to understand how to set up to start with, but now it is just offered as a service provided, you can just pay into it and it is automatically done for you. So you do not need that technical understanding to start with now. Anybody can use a V.P.N. to do anything.*<sup>120</sup>

No work is being done by Government at the current time to consider and address any challenges posed by VPNs. The Minister for Sustainable Economic Development advised the Panel that prohibiting VPNs would be impractical, describing the idea as a “*non-starter*”.<sup>121</sup>

VPNs are legal in the U.K., however, under the OSA platforms have responsibilities to prevent children from bypassing safety precautions. Therefore, where certain platforms deliberately target U.K. children and promote VPN use, they could face enforcement action, including significant financial penalties.<sup>122</sup> There is no equivalent requirement in Jersey.



#### **FINDING 23**

Internet Service Providers in Jersey cannot block content on various websites, therefore internet users in Jersey may be able to access content that would be blocked by networks in the U.K.



#### **FINDING 24**

Virtual Private Networks (VPNs) and proxy internet protocol (IP) addresses create further challenges for enforcing jurisdictional boundaries on the internet as users can circumnavigate restrictions from the region they are in. In the U.K. the Online Safety Act creates obligations for platforms to prevent children bypassing safety precautions, but there is no equivalent obligation in Jersey legislation.



#### **RECOMMENDATION 10: Key Recommendation**

The Minister for Sustainable Economic Development should explore and undertake a public consultation on the development of legislation that would require all on-Island internet service providers to introduce network-level filtering that is active by default and customisable by the contract holder.

<sup>120</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.29

<sup>121</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.19

<sup>122</sup> <https://www.gov.uk/government/news/keeping-children-safe-online-changes-to-the-online-safety-act-explained> (accessed 28/08/2025)

## Platforms' own rules and guidelines

Social media and digital platforms can play a role in protecting children from online harms through their internal rules, guidelines, and safety features. Platforms can implement their own systems to safeguard young users, but some jurisdictions will attempt to shape these measures through legislation (such as the U.K. with the OSA) and regulatory oversight (e.g. Ofcom).

Platforms sometimes face criticism about the robustness of their safety features. One submission to the Panel emphasised the opaque influence of algorithms and suggested that the underlying business models of social media companies significantly shape their behaviour:

*We must be clear that social media is not the same as the internet. The business model of social media platforms is about 'eyeballs' and attention. They are addictive, they are programmed for engagement (not control), and they are full of hidden rewards, incentives and dark patterns. None of that is accidental, it is by design.*

*As an illustration, in 2017, a document was released that revealed how Facebook was offering advertisers the opportunity to target 13-17 year olds across its platforms (which includes Instagram), particularly during moments of 'vulnerability'. This gives one small but significant insight into the way in which these platforms are run.*

*It is worth noting that there are two broad groups of people who do not allow their children to use social media – the product designers, and the product researchers.*

*It is the algorithms, the addiction, and the manipulation which are at the heart of the harms. With recent figures showing that AI fuelled bots make up over half of internet traffic, this is a problem that is growing rapidly.<sup>123</sup>*

The Panel has not undertaken a comprehensive desktop review of the most popular social media platforms community guidelines or terms of service, however, we did attempt to contact several companies to establish if users in Jersey would be classed differently to those in the U.K.

[TikTok](#) was the only company to provide a formal submission to the Panel and confirmed that they had a global approach to content safety, which was underpinned by their site's Community Guidelines and Terms of Service.

*All users are subject to our Terms of Service and Community Guidelines, regardless of where they are based. As such, the current user experience for individuals based in Jersey, including users aged 13-18, is the same as other regions like the UK.<sup>124</sup>*

TikTok's submission explained their approach included an age graduated experience:

*It is important to note that TikTok's Terms of Service and Community Guidelines often exceed legislative requirements. TikTok is a newer platform than many of the traditional social media companies and as such, many aspects of the platform's design, policies and approach are aligned with those of international legal frameworks such as the Online Safety Act and Digital Services Act.*

*For example, TikTok takes an age-appropriate, graduated experience to its service. Users aged 13- 15 have a different experience to those 16-17, and those who are over*

---

<sup>123</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>124</sup> [Written Submission – Online Harms Review - TikTok](#)

*18. For example, users under 16 are prohibited from accessing direct messages. Users 16-17 are able to access direct messages, but they are turned off by default. Other features like the ability to livestream are prohibited for all users under 18.*

*These features, alongside industry leading measures like a default 1 hour screen time limit for under 18s, and wellbeing tools including guided meditation, are part of the default TikTok experience for minors.<sup>125</sup>*

The House of Commons' Science, Innovation and Technology Committee (the 'Select Committee') undertook a review of '[Social media, misinformation and harmful algorithms](#)' and published a report in July 2025. During the evidence sessions representatives from Meta, TikTok, X and Google all provided verbal evidence which identified the different approaches the companies had to addressing safety online, both generally and (as per the Select Committee's review focus) in the specific case of the spread of online misinformation following the murders in Southport in July 2024. Further details of this report are shared in the section on '[Misinformation](#)'.

#### **FINDING 25**



Social media and online platforms typically enforce 'terms of service' or 'community guidelines' that users must follow to maintain access and help ensure a safer, more respectful environment for everyone, however, each platform or company will define its own unique set of rules which leads to different standards across platforms. Whilst TikTok has confirmed that it has a global approach and that users in Jersey receive the same user experience as those in other jurisdictions, this is not the same for every social media or digital platform.

#### **FINDING 26: Key Finding**



The absence of government-defined standards or regulations in Jersey for platform-led content governance suggests an implicit acceptance that decisions about potentially harmful content, particularly affecting children, are determined by corporate policies rather than by local legislative oversight or public authority.



#### **RECOMMENDATION 11**

The Government of Jersey should clarify its position on legislating for online content governance, with particular emphasis on material that may be harmful to children. Doing so would signal whether the Island intends to establish its own regulatory standards or continue to rely on platform-led policies.

---

<sup>125</sup> [Ibid](#)

## During school time

Schools and places of education have different responsibilities with regards to protection of children and young people from online harms. The Minister for Education and Lifelong Learning advised the Panel that it was a dual aspect, namely:

- to provide safe access at schools to the internet for teaching and educational purposes; and
- an education role itself, i.e. how to behave online and understand what is safe online.<sup>126</sup>

The Minister also stated the importance of dealing with any issues when they arise in conjunction with parents and that schools had been “*drawn into the world of mobile phones*” but that they had done an “*enormous amount of work to try and deal with that issue as well*”.<sup>127</sup>

When asked what the top three protections that children in Jersey currently have from online harms, the Minister for Education and Lifelong Learning responded by referring to protections delivered through schools:

*The top 3 are the software that overlays our schools. I think the other one is the fact that it is part of the Schools Review Framework. It has become front and centre to what we are doing. I suppose the third one is that there is a mobile phone policy in every school.*<sup>128</sup>

Throughout this Panel’s review the Minister for Education and Lifelong Learning has emphasised the robust procedures that are in place within schools already and the work schools do for educating on this topic. He advised the Panel that “*schools, as corporate parents, are responsible for keeping children safe online, and technical monitoring is essential for achieving this. Various safeguarding measures are in place, including software designed to mitigate harm in digital environments. These systems aim to support teachers in managing online risks and promote safer digital experiences for students*”.<sup>129</sup>

### Safe internet access at schools

The School Review Framework has also been referenced as a “*pivotal part*”<sup>130</sup> of the review system, which is used to evaluate schools’ online safety procedures. Schools statutory responsibility for safeguarding is set out in [Appendix 5](#) of the Jersey School Review handbook. The document explains that the Department for CYPES are signatories to the Memorandum of Understanding with the Safeguarding Partnership Board, under the authority of the Chief Minister. The Panel understands that a frequency of a Jersey School Review is every 3-4 years.<sup>131</sup>

Amidst others, there is a specific section in the appendix relevant to online safety, which states the responsibilities for schools:

---

<sup>126</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.4

<sup>127</sup> [Ibid](#), p.4

<sup>128</sup> [Ibid](#), p.3

<sup>129</sup> [Letter – Online Harms Review – Minister for Education and Lifelong Learning – 27<sup>th</sup> May 2025](#)

<sup>130</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.5

<sup>131</sup> <https://www.gov.je/education/schools/childlearning/pages/jerseyschoolsreviewframework.aspx> (accessed 26th August 2025)

*Online safety - schools will:*

- oversee and monitor the safe use of technology when children are in their care and take action immediately if they are concerned about wellbeing
- ensure that all staff receive appropriate online safety training that is relevant and regularly updated
- ensure there are mechanisms in place to support young people and staff facing online safety issues
- implement online safety policies and acceptable use policies, which are clear, understood and respected by all
- educate young people, parents and the school community to build knowledge, skills and capability in online safety
- monitor how the school is portrayed online by parents, children and staff- and demonstrate how this is monitored
- not request for a website to be unblocked or application installed unless a risk assessment has been completed.

132

The Minister for Education and Lifelong Learning also advised the Panel about the [Keeping Children Safe in Education](#) (KCSiE) statutory guidance. There is a section in the KCSiE guidance specifically relevant to Online Safety, this recognises the 4Cs referenced earlier.

In one [written response](#) to the Panel from the Minister for Education and Lifelong Learning there was a reference to the Keeping Children Safe in Education Law 2022, however, this is U.K. based legislation and is not extended to Jersey, therefore the Panel queried this and clarification was provided that the [Children and Young People \(Jersey\) Law 2022](#) provided the “*legislative lever*” in Jersey that provided the duties for Ministers and Chief Officers in relation to safeguarding.<sup>133</sup>

The CYPES ‘[Online Safety Policy](#)’ is dated August 2021 and the Panel learned during a public hearing that it was under review. The Minister described that it should be treated as a “*live document*” and a “*risk assessment*” and kept under constant review in order to keep up with changes in the environment and impacts that this had on risk.<sup>134</sup> The Panel found that, despite a reference to an ‘online safety incident’ there was no current definition of this, however, the Head of Governance and Digital for CYPES confirmed that it would be in the next revision of the policy.

The Panel also discovered that CYPES don’t keep a departmental record of ‘online safety incidents’ and was advised that this was because individual schools were the data controllers. In response to further queries, the Minister indicated that this was not a problem for CYPES not to have this data, but clarified that it was something that “perhaps it is something we do need to look at”.<sup>135</sup> It was suggested that this data could help the department get an understanding of the challenges, however, it was confirmed that any serious incidents would

---

<sup>132</sup> Jersey School Review Handbook 2025:

<https://www.gov.je/SiteCollectionDocuments/Education/P%20Jersey%20Schools%20Review%20Framework%2020191001%20PH.pdf> (accessed 21/08/2025)

<sup>133</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.14

<sup>134</sup> [Ibid](#), p.15

<sup>135</sup> [Ibid](#), p.18

be reported on S.I.M.S (school information management system) and any safeguarding incidents would be highlighted as part of the school's safeguarding audit.<sup>136</sup>

Furthermore, the current policy describes that “*CYPES distributes daily reports to state schools about the suspicious search queries made on Google the previous day*”<sup>137</sup>. However, it was confirmed that the manual-based process was no longer in use, and the Panel was advised that there were now real-time alert flags that automatically flag issues to the safeguarding lead in a school.<sup>138</sup> The Panel was advised that a revised Online Safety Policy would be published to reflect updated operational and best practice.<sup>139</sup>

The Panel found that the online safety filters used by CYPES only functioned on devices connected to the school's network or Wi-Fi. Therefore, if someone accesses the internet using mobile data, the CYPES filtering system does not apply.

The [Online Safety Policy](#) notes that there is no legal requirement for schools to have an internal technical monitoring system, as there is in the U.K. The Panel explored this in enquiries with the Minister for Education and Lifelong Learning, who confirmed that all of the Government of Jersey provided schools had an internal technical monitoring system and that funding for this was provided centrally by Digital Services (rather than through CYPES).<sup>140</sup>

The Minister highlighted the following key monitoring responsibilities, namely:

1. The use of filtering and monitoring systems in schools to reduce children's exposure to harmful online content and supports early identification of potentially concerning digital behaviour;
2. Online safety incidents are monitored, recorded and followed up;
3. Regular safeguarding audits and self-evaluations for schools;
4. Role of the Jersey School Review Framework will consider how well schools met their duties to safeguard children (each school should be reviewed on a 3-4 year cycle);
5. Online safety is delivered by schools in Computing and PSHE lessons;
6. 'Education for a Connected World' framework has been adopted by most primary schools, which focusses on 8 different aspects of online education; and
7. The role of the Online Safety Lead in a school.

The Panel asked for more details about the software that was in place to provide monitoring in schools. The Panel learned that this is provided by:

- Lightspeed Filter and Lightspeed Alert, which provide online filtering and reporting. The Panel learned that Lightspeed Filter also protects mobile devices connected to the wi-fi in schools from harmful content; and
- Activian.<sup>141</sup>

---

<sup>136</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.19 **Note:** during the factual checking process it was clarified that in practice, safeguarding concerns are recorded in 'MyConcern' which is the designated platform for managing and escalating safeguarding issues in schools.

<sup>137</sup> [Research – Online Harms Review – Government of Jersey, CYPES Online Safety Policy – August 2021](#)

<sup>138</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.21

<sup>139</sup> [Ibid](#), p.15 and p.20

<sup>140</sup> [Letter – Online Harms Review – Minister for Education and Lifelong Learning – 10<sup>th</sup> March 2025](#)

<sup>141</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.3



The Head of Governance and Digital, CYPES explained the software to the Panel in a public hearing:

*The 2 systems that are in place are real time, so it acts as an early detection method to pick up anything immediately. These are logged as alerts. They go directly to the designated safeguarding leads, who then can act immediately as they occur. They are continually reviewed, the software applications, with emerging technologies such as A.I. (artificial intelligence), for example, to then look at that to see whether they are still the best possible filtering systems in place, because they change, of course, over time with those emerging risks.*<sup>142</sup>

The Panel was also interested to learn about the safeguarding audits used in schools, which were used to assess the effectiveness of measures in place to mitigate risks from online harms:

*There are annual safeguarding audits across all schools that are designed to help improve safeguarding in schools. It is used as a self-evaluation tool for schools to look at all areas of safeguarding, but there is a significant area within that that relates to online harm and digital safety. So the department work with the schools annually to make sure that everything they have is robust and in place.*<sup>143</sup>

The Panel was advised that the outcomes of the audits were discussed between the school and CYPES and it was emphasised that these were used as a self-improvement tool.<sup>144</sup>

The Panel understands that the responsibility for online safety in a school is that of the Designated Safeguarding Lead (DSL), but they may appoint a separate Online Safety Lead. The Panel was advised about that role:

*Key responsibilities include managing reports of online safety issues, contributing to policy development, and promoting online safety awareness across the school community. The role also involves coordinating with curriculum leaders to embed online safety into teaching, ensuring staff are trained in incident response procedures, and providing or sourcing training for staff, parents, and pupils. The Online Safety Lead works collaboratively with technical and pastoral teams and must undertake regular, up-to-date training to stay informed about digital risks related to content, contact, conduct, and commerce, as defined in Keeping Children Safe in Education.*<sup>145</sup>

The Panel has noted that some of the references in the KCSiE guidance refer to U.K. information and guidance, for example: [The National Crime Agency's CEOP Education team](#); [www.saferinternet.org.uk](http://www.saferinternet.org.uk); [www.internetmatters.org](http://www.internetmatters.org); [Childnet Online Safety Resources](#). If the Jersey specific guidance relies on U.K. based information, the Panel raises concerns regarding a potential divergence between the online regulatory environments of the U.K. and Jersey following the implementation of the U.K.'s OSA, noting that internet users in Jersey may not fully benefit from the broader protective measures introduced under the OSA.

There is nothing in the KCSiE policy about educational technology (EdTech) and the Online Safety Policy says to “Only use websites and web based applications with students when they have been risk assessed and you have read and reviewed the terms and conditions and are satisfied that they do not pose a significant online safety or data protection risk”. EdTech is

---

<sup>142</sup> [Ibid](#), p.5

<sup>143</sup> [Ibid](#), p.12

<sup>144</sup> [Ibid](#), p.42

<sup>145</sup> [Letter – Online Harms Review – Minister for Education and Lifelong Learning – 27<sup>th</sup> May 2025](#)

the blend of teaching practices and technological tools which are designed to enhance learning. Benefits of EdTech can include adapting personalised learning, engagement, accessibility and efficiency. However, there are challenges and considerations, not least the protection of students' data and online safety. Also, there are aspects such as ensuring that teachers are suitably trained, and that any digital divide is considered (for example, if some students do not have devices or internet connection at home).

The [Children and the Digital World](#) report published by the Government of Jersey in 2021 identified that: *"the need for investment in IT equipment and in maintaining education practitioners' levels of digital literacy was identified as it is essential that educators are proficient in the safe delivery of digital education"*.<sup>146</sup> During the review the Panel also learned that the Digital Services department (not CYPES) was responsible for running the network, upgrading the wi-fi and providing the funding for the filtering and monitoring services to schools, however, there was £400,000 of funding across all schools to spend on devices.<sup>147</sup>

#### FINDING 27



Schools serve a dual role in relation to protecting children from online harms: to safeguard students and, also, educate them about how to stay safe online. The Minister for Education and Lifelong Learning also advised that schools had to work with parents and had been "drawn in" to the world of mobile phones.

#### FINDING 28



School statutory responsibilities for safeguarding are set out in Appendix 5 of the School Review Handbook and this includes responsibilities related to online harms. School reviews under the School Review Framework are conducted every 3-4 years.

#### FINDING 29



The current CYPES Online Safety Policy is dated August 2021 and the Panel established that several aspects detailed within it are no longer operational practice. It was confirmed that procedures have since been updated and improved, and that the policy itself is undergoing review. The Panel was advised that a revised version will be published to align with the updates.

#### FINDING 30



The Online Safety Policy and safety features such as filtering and monitoring software are only applicable to devices that are connected to the school network or wi-fi. If an individual uses data on a mobile device to access the internet, the CYPES filtering software will not apply.

#### RECOMMENDATION 12



The Minister for Education and Lifelong Learning and Minister for Children and Families should ensure the timely publication of the updated CYPES Online Safety Policy and share it with the Scrutiny Panel at the earliest opportunity to facilitate informed discussion and review. The revised Policy should explicitly address the appropriate access to online and digital content for children and young people attending school and educational settings, including the risks associated with mobile data use.

<sup>146</sup> [Children and the Digital World](#), Government of Jersey, May 2022, p.14

<sup>147</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.34 **Note:** during the factual checking process it was clarified that the £400,000 of funding is ring-fenced for the replacement of aging hardware and cannot be used at the school's discretion for unrelated purposes.



### RECOMMENDATION 13

The Minister for Education and Lifelong Learning should evaluate whether the U.K. based online safety guidance referred to in Jersey's Keeping Children Safe in Education policy suitably reflects Jersey's regulatory environment. Given the reliance on U.K. based resources, and the potential divergence following the U.K.'s Online Safety Act, Jersey-specific measures should be developed to maintain effective protection for internet users.

### Mobile phones and smartphones in schools

Many of the public submissions that the Panel received as part of this review related to the use of mobile phones in schools (these can all be read on the Panel's review pages, [here](#)). As outlined above, the CYPES Online Safety Policy does not include controls over online content accessed through a digital device accessing a mobile data plan.

When the Panel questioned the Minister for Education and Lifelong Learning on 16<sup>th</sup> May 2025, he acknowledged widespread concerns about children accessing harmful content via mobile devices and emphasised that most Jersey schools already had strict policies in place and stated that approximately 96% of schools had effectively eliminated mobile phone use during the school day. However, the Minister also raised concerns about the practical challenges schools faced in monitoring and enforcing students' mobile phone usage and highlighted that it was "*impossible*" for schools to do this once students had left the premises and said that there were already policies that restricted student access during school hours.<sup>148</sup>

At the time of the public hearing with the Panel, rather than advocating for a blanket ban, the Minister praised the collaborative approach schools have taken, working with students and parents to develop tailored policies. The Minister suggested that announcing a ban could make for a good headline but would be "*meaningless*" without the cultural change and community support. He stressed the importance of educating young people about responsible phone use and involving them in the process, rather than imposing top-down rules.<sup>149</sup>

In contrast to this approach, the Panel received a written submission from Dr. Chris Edmond, a member of the Health Professionals for Safer Screens group, who advised that:

*It does appear that in the case of smartphone use by children (and particularly in the school environment) there is increasing evidence of hazard and potential harm, yet the appropriate approach to risk mitigation (i.e. to eliminate the hazard where possible) has been set aside for a preference to place administrative controls (such as education and recommendations of individual behaviour change). In the longer term, I am sure that improved product design (i.e. engineering controls as per the hierarchy) will be possible but for the time being it appears that duties under the health and safety legislation are not being adequately balanced against other rights of the child.<sup>150</sup>*

There has been considerable interest in this subject and in March 2025 the States Assembly was advised that Article 35 of the Education (Jersey) Law imposes statutory duties on headteachers in relation to the management of behaviour and discipline which could arguably apply to the use of mobile phones in schools. It was explained that there was also a customary or common law duty of care on the part of the Minister for Children and Families (sic) at school,

<sup>148</sup> [Ibid](#), p.25-26

<sup>149</sup> [Ibid](#), p.26

<sup>150</sup> [Written Submission – Online Harms Review – Dr. Chris Edmond](#)

which may give rise to a claim in negligence for an alleged breach and risk needed to be assessed.<sup>151</sup>

The Minister for Education and Lifelong Learning confirmed that during school hours, teachers were in *loco parentis* and, therefore, schools were responsible for monitoring mobile phone use.<sup>152</sup> The Minister opined that:

*I think the monitoring in school is probably much, much better than outside of school. Is it perfect? I would suggest no because I do not know if it can be, but is it sufficient ... I mean, that is a really difficult one. I would say yes, but it can always be improved. One feature of good schools and good education is they are self-improving, and you look at where there are issues.*<sup>153</sup>

During the public hearing in May 2025 the Minister spoke further of the culture of improvement and suggested that policies needed to be treated like risk assessments and considered as ongoing. He cautioned against adopting a centralised mobile phone policy, suggesting it might create a false sense of resolution and discourage the continued, collaborative effort needed to address the evolving challenges of mobile phone use in schools.<sup>154</sup>

When the Panel initiated this review in early 2025 each school had its own mobile phone policy, but there was no centralised CYPES direction on the matter. However, one month after the public hearing, in June 2025 the Minister for Education and Lifelong Learning wrote a letter to parents and advised that from the start of the school term in September 2025 there would be updated rules relating to mobile phone use in all Government provided and Government fee-paying schools.

The Panel notes that this approach will theoretically create a fairly consistent approach across Government of Jersey schools, however, queries if, or how, CYPES will measure the impact of the changes and collect feedback from students and parents.

In July 2025 the Panel was advised about some of the views that had been shared with the Office of the Children's Commissioner in relation to mobile phone use:

*Some of our advisory panel expressed anxiety about not being able to actually have their phone on their person, even if switched off. They tended to talk about what happens in an emergency. What happens if I really need to contact my parents? But some also felt that it was kind of a sign of mistrust in them to adhere to a no phones policy in school and that they were not trusted to have them without them actually being physically removed from them. They also very clearly raised the fact that they were not consulted about this direction, that this was something that simply they were informed of but they were not asked about.*<sup>155</sup>

---

<sup>151</sup> [Hansard - States of Jersey Assembly, 18<sup>th</sup> March 2025](#), p.82

<sup>152</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.28

<sup>153</sup> [Ibid](#), p.5

<sup>154</sup> [Ibid](#), p.19 & p.31

<sup>155</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.3 **Note:** in the factual checking process, it was highlighted that this reference to the advisory panel refers to the youth advisory panel, made up of children and young people.

These reflections underscore the importance of involving children and young people in decisions that directly affect their daily lives, particularly when it comes to policies around mobile phone use.

In a report published by the Digital Futures for Children centre which reviewed evidence collected in relation to smartphone policies in schools, it was found that restrictions did not deal with the source of some risks posed to children by digital technology:

*Crucially, talk of ‘bans’ closes down the deeper conversations society needs to have about the best interests of children in a digital age and lets the profit hungry tech sector off the hook. It remains the case that the devices are configured in ways that support the commercial interests of the products and services that they carry. It is a society-wide duty to do more to prevent the design and deployment of services that are deliberately designed to distract.*<sup>156</sup>

Therefore, while implementing stricter mobile phone policies may help reduce certain risks (as noted in the Safer Screen submission) and responds to parental calls for action, it does not tackle the broader, systemic issues rooted in the design of digital technologies. These include the commercial motivations behind addictive features and harmful content, which require coordinated regulatory and societal responses beyond the scope of school interventions.

In one submission to the Panel, it was suggested that the public debate about online harm focusses wrongly on hardware devices and calls to ban smartphones. It was suggested that this was a limited view, as “*devices are at one end of the digital communications chain that has websites and online platforms at the other end, linked by Internet Service Providers through mobile data and broadband connections*”.<sup>157</sup>

This theme was echoed in the evidence provided to the Panel by the Information Commissioner. Whilst acknowledging that a smartphone ban was “*a step*”, he stated that it would be a mistake to think that it would resolve the issue and emphasised that children and young people are “*digital natives*” and rely on digital tools in a way that older generations do not.<sup>158</sup> The written submission from the Office of the Information Commissioner stated:

*Restricting access may not, in our respectful view, wholly address the underlying challenges and may not be entirely practical or effective in isolation and overly restrictive measures could hamper children’s own education in terms of their developing essential digital skills which they will undoubtedly need to navigate the world in which we live.*<sup>159</sup>

In a submission to the Panel, the Principal of Highlands College said that access to and use of smartphones was “*ubiquitous*” among students and staff on the campus. With regards to their use for education, it was explained that:

---

<sup>156</sup> Miriam Rahali et al., ‘[Smartphone policies in schools: What does the evidence say?](#)’, Digital Futures for Children Centre, September 2024, p.26

<sup>157</sup> [Written Submission – Online Harms Review – Jon Tarrant – 23<sup>rd</sup> May 2025](#)

<sup>158</sup> [Transcript – Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.16

<sup>159</sup> [Written Submission – Online Harms Review - Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)



*Views on the productive use of smartphones for educational purposes are mixed. There is evidence of productive use in lessons, enabling students to access materials, engage in online quizzes, and capture examples of their learning. However, there are also instances of students being distracted by notifications. For many students, their smartphone is their only personal digital device, and they are keen to always have it in their possession. Restricting access to their mobile phones may reduce their equitable access to productive web/app-based educational services.*<sup>160</sup>

While the Panel will explore digital literacy within the curriculum in the following section, it wishes to highlight key findings from the report published by the Digital Futures for Children centre. The report emphasises that smartphone policies in schools should be closely aligned with a comprehensive digital literacy curriculum:

*Smartphone policies should be underpinned by a digital literacy curriculum that encompasses privacy, safety, genre, learning outcomes and monitoring, and embedded in wider EdTech policies to bridge school and home use.*<sup>161</sup>

Furthermore, Public Health Jersey's submission to the Panel recommended that the Government develop policies across schools to minimise phone use during the day.

***School mobile phone policies*** - *Develop a policy across schools to prevent or minimise use during the school day, especially for younger pupils. France's national ban up to age 15 across all schools offers a potential model Jersey could adopt or adapt.*<sup>162</sup>

Public Health's submission also advocated for providing guidance around age-appropriate use of screens and co-designing screen use policies with schools, parents, students and communities.

#### FINDING 31



During the course of the review, the Minister for Education and Lifelong Learning announced that there would be more restrictions put in place for students' use of mobile phones within all Government of Jersey provided and fee-paying schools from September 2025.

#### FINDING 32



Restrictions or bans on mobile phone use in educational settings can be a way to reduce potential risks, such as exposure to inappropriate content and excessive screen time. However, these measures do not address the root causes related to harmful content itself and may inadvertently limit students' access to educational resources and opportunities to develop essential digital skills.



#### RECOMMENDATION 14

The Minister for Education and Lifelong Learning should engage with key stakeholders to review mobile phone policies and guidance for schools and, also, develop mechanisms to evaluate the effectiveness of the policy changes, ensuring they achieve their intended outcomes and provide meaningful protection for children in practice.

<sup>160</sup> [Written Submission – Online Harms Review – Highlands College](#)

<sup>161</sup> Miriam Rahali et al., '[Smartphone policies in schools: What does the evidence say?](#)', Digital Futures for Children Centre, September 2024, p.25

<sup>162</sup> [Written Submission – Online Harms Review - Public Health Jersey](#)



### **Educating about online harms**

As referenced above, the Minister for Education and Lifelong Learning indicated that one of the key roles that schools have in relation to online harms and safety is providing relevant information to educate about the issue. In the information provided to the Panel it was confirmed that this education is embedded within the Jersey curriculum, particularly through computing and PSHE (Personal, Social and Health Education) in both primary and secondary schools. The Panel was advised that some schools have also developed their own digital literacy programmes. As detailed in Appendix 5 of the [School Review Framework Handbook 2025](#) (which outlines statutory safeguarding responsibilities), schools have to educate young people, parents and the school community to build knowledge, skills and capability in online safety.

When asked whether the current provision was adequate, the Minister acknowledged that the curriculum must evolve to keep pace with a rapidly changing world, citing developments in artificial intelligence as a key example.<sup>163</sup>

The Head of Governance and Digital of CYPES advised that:

*Obviously, we launched the digital education strategy in 2023 and one of the particular strands in that is looking at teacher training and the standardisation on that to make sure there is parity across all schools and that everyone, both teachers and students, are at a sufficient level to adequately teach those pupils what the safeguards are that are required to be a digital citizen, an effective digital citizen, and to go into employment. Because ultimately our children are the ones that are going to run the country at some point.*<sup>164</sup>

The Panel asked how much money, if any, was spent by Government of Jersey schools on specific online safety training. The Panel was advised that there was no specific online safety training budget, however, there had been training provided to teachers funded through the CYPES central training budget in the sum of £6,000, however, it was advised that the schools themselves would have funded a lot of training themselves.<sup>165</sup> The Minister said that they want to recognise where more central training is needed and target those specific areas:

*It is not just simply an external amount of money, it is about enabling staff to learn from each other. Schools do that brilliantly themselves, and we need to encourage that more centrally.*<sup>166</sup>

The Panel queries if this absence of funding and consistency is suitable for a matter that is a statutory safeguarding responsibility.

In correspondence from the Minister for Education and Lifelong Learning, it was noted that “*additional funding provided by external sponsorship*”<sup>167</sup> had been secured to deliver online safety training in schools. The Panel subsequently requested details regarding the amount and source of this funding. However, this information has not been made available to us as

---

<sup>163</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.8

<sup>164</sup> [Ibid](#), p.8

<sup>165</sup> [Ibid](#), p.33

<sup>166</sup> [Ibid](#), p.34

<sup>167</sup> [Letter – Online Harms Review – Minister for Education and Lifelong Learning - 10<sup>th</sup> March 2025](#)

part of the review process. The Panel would be interested to understand more about the external sponsorships which are supporting schools to deliver online safety training.

The Panel made some enquiries about both the age-appropriate approach to online safety and, also the approach to teaching online safety to students with additional needs and special educational needs (SEN). With regards to supporting vulnerable groups, the Children's Commissioner has said that relying exclusively on digital safety education in schools is not going to meet the needs of many vulnerable groups.<sup>168</sup> This aspect has been briefly touched on in the earlier report section '[Are children and young people considered to be more vulnerable to potential online harms?](#)'.

The Minister for Education and Lifelong Learning recognised that there was an additional challenge around the provision of SEN advised that schools had an understanding of the needs of its pupils on an individual level, particularly for children with SEN or where there was a record of need. He explained that schools understood the importance of meeting this challenge in order to protect the children from risk.<sup>169</sup>

### FINDING 33



Education about online safety and protection from online harms is a statutory responsibility for schools and is incorporated within the Jersey curriculum in both primary and secondary schools and some schools have also developed their own digital literacy programmes. However, there is no dedicated budget for online safety training in schools. A sum of £6,000 was allocated from the central CYPES training budget, with additional training for teachers funded directly by schools. The Minister has highlighted peer learning among staff as a valuable resource.

### FINDING 34



There are challenges in delivering age-appropriate and SEN-sensitive online safety education, with schools reportedly tailoring approaches to individual pupil needs.

### RECOMMENDATION 15



The Minister for Education and Lifelong Learning should prioritise consistency in the delivery of online safety education across all schools with consideration about the suitability of funding for this statutory requirement. This includes ensuring that teacher training is standardised and aligned with the digital education strategy to provide equitable learning experiences. Additionally, particular attention should be given to the development of tailored approaches for students with Special Educational Needs.

<sup>168</sup> [Transcript – Online Harms Review – Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.9

<sup>169</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.11

## Youth clubs

The [CYPES Online Safety Policy](#) is relevant for youth services as well as schools. The Panel asked the Minister for Children and Families how the Jersey Youth Service fulfilled its responsibilities, as per the policy, to “*oversee and monitor the use of technology when children are in their care*”. The Minister responded to say that the Jersey Youth Service does not currently provide any devices for children and young people to access the internet, so there is currently no need to oversee and monitor the use of technology when attending a youth club.<sup>170</sup>

The Minister has not confirmed if there is Lightspeed Filter software in place to filter content when it is accessed through the CYPES wi-fi<sup>171</sup>, however, as with schools there is the challenge of accessing content through mobile data and there is no way for this to be filtered and controlled by CYPES.

The Panel received one submission from a member of the public which stated that children had been exposed to inappropriate content whilst in attendance at a youth club:

*Finally, I am distraught, but want to make you aware that a few children from my eldest child's peer group (age 10/11) were recently exposed to videos of explicit and sexual nature on another minors smart phone whilst at a youth club. Whilst I can refrain from buying my children their own smart phone, I can only encourage them to not look at others when given opportunity but am also well aware of the documented addictive traits of smart phones.*<sup>172</sup>

As previously mentioned in relation to the topic of mobile phone use in schools, the Panel has noted that there is a customary or common law duty of care on the part of the responsible Minister at school, therefore, the Panel questions if this would also transfer to a youth club. In a submission to the Panel from [Jon Tarrant](#), he questions: *Is the act of not providing devices sufficient grounds for obviating Youth Clubs' duty of care?*

### FINDING 35



The Minister for Children and Families has stated that there is no need to oversee and monitor the use of technology when attending a youth centre as the Jersey Youth Service does not currently provide any devices for children and young people to access the internet. The Panel is concerned that the absence of provided devices does not remove the duty of care owed by youth services when children are in their care.

### RECOMMENDATION 16



The Minister for Children and Families should ensure that any revised CYPES Online Safety Policy explicitly addresses the appropriate access to online and digital content for children and young people attending youth clubs, including the risks associated with mobile data use. This should be recognised as a distinct safeguarding responsibility within youth services.

<sup>170</sup> [Letter – Minister for Children and Families – 10<sup>th</sup> March 2025](#)

<sup>171</sup> [Ibid](#)

<sup>172</sup> [Written Submission – Online Harms Review – Anonymous 9](#)

## Children in the care of the Minister

The Panel was interested to understand how online safety was approached for children in residential care, as the [CYPES Online Safety Policy](#) did not extend to cover children's residential homes. The Panel was advised by the Minister for Children and Families that the Residential Service has a system called Sophos which is used to monitor wi-fi use and filter or block harmful content from any device connected to the wi-fi. It was confirmed that internet rules and expectations are set out in an easy-to read guide which was provided to residents.<sup>173</sup>

In a letter to the Panel in March 2025, in response to a query about the policies and procedures in place for filtering and monitoring content accessible on mobile devices of children in the care of the Minister, it was confirmed that Children's Social Care were "*undertaking a wide-ranging review of all of our policies across the whole service, including all those in the residential estate, and these are currently in draft*".<sup>174</sup> However, with regards to current arrangements the Panel was advised that children's individual care planning documents and safety plans are used to address any vulnerabilities and safeguards in relation to online harm. Children's internet use is monitored by residential staff, and it was confirmed that they can check children's phones for any evidence of risk. Keyworker sessions are used to discuss safety and relationships.<sup>175</sup>

During a public hearing on 23<sup>rd</sup> May 2025 the Minister for Children and Families advised that all but two of the Children's Residential homes had filtering software in place and it was clarified that those without the internet filtering were the short break homes, which were used to provide overnight breaks for children with significant learning disabilities. The Minister stated:

*I have only recently become aware of that and I have been assured that the 24/7 cover is sufficient at this stage, but we are about to bring in filtering software. The problem that we have in all these locations is that children have smartphones and switch on to 4G and completely bypass any controls that we put in place. So the filtering that we put in only achieves something when they are on our network and there is very little we can do when they have switched on to another network; that is the 4G network.*<sup>176</sup>

Following the public hearing the Minister for Children and Families provided the Panel with some further information to explain the policies for mobile phones and internet use in Children's Residential Settings. He confirmed that no mobile phones were allowed in the short breaks homes, but where young people did bring devices (such as iPads) they were subject to parental controls and were not left unsupervised with them. The Minister reiterated that "*along with the rest of the estate, these Short Breaks homes are in line to be fitted with new filtering systems. The project plans to implement these systems are currently under consideration*".<sup>177</sup>

---

<sup>173</sup> [Letter – Minister for Children and Families – 10<sup>th</sup> March 2025](#)

<sup>174</sup> [Ibid](#)

<sup>175</sup> [Ibid](#)

<sup>176</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.23

<sup>177</sup> [Letter – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

The Panel was advised in June that “a review of online safety systems across schools and children’s care homes has been undertaken, with a project now in progress to enhance protective measures and ensure consistency in safeguarding across settings”.<sup>178</sup>

The Panel was advised about a bespoke data protection training programme that had been developed for staff in Children’s Social Care in 2024, it was confirmed that this had been delivered to all staff in the social work teams and was anticipated to have been delivered to the residential aspect of the service by the end of March 2025.<sup>179</sup>

The Panel also heard that as part of the redevelopment of the online safety policy there would be consideration of the introduction of mobile device management platforms that would give further insight into safeguarding children in care.<sup>180</sup>

The Panel has collected limited evidence in relation to the protections in place for children in foster care, but has been advised that:

*Foster carers are trained in safeguarding children, which includes how to keep children safe when using mobile phones or the internet. Foster carers are required to have parental controls on their own devices, as well as children’s devices so that inappropriate material cannot be accessed. Foster carers are also expected to have regular discussions with children in their care and record in daily logs when these have taken place.*<sup>181</sup>

General Comment No. 25 specifically references that it is important that children separated from their families, including those that may be placed in foster care, have access to digital technologies. However it states that this should be balanced with the need to protect children in cases where parents or other family members or caregivers, whether physically present or distant, may place them at risk:

*States parties should consider that such risks may be enabled through the design and use of digital technologies, for example, by revealing the location of a child to a potential abuser.*<sup>182</sup>

## Corporate Parents

It is worth noting that corporate parents are defined in the schedule of the Children and Young People (Jersey) Law 2022 and include the Chief Minister and Ministers, a department or unit of administration established on behalf of the States, the parishes, The States of Jersey Police Force, the Jersey Probation and Aftercare Service, schools, nursery schools, and day care accommodation, and certain bodies operating at arm’s length from the States.

There is a differentiation between the responsibilities the States of Jersey has to all children, compared to the additional responsibilities imposed for corporate parenting. Per part 6 of the Children and Young People (Jersey) Law 2022, corporate parenting is only applied to individuals who are:

- Looked after children;

---

<sup>178</sup> [Letter – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

<sup>179</sup> [Letter – Minister for Children and Families – 10<sup>th</sup> March 2025](#)

<sup>180</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.36

<sup>181</sup> [Letter – Minister for Children and Families – 10<sup>th</sup> March 2025](#)

<sup>182</sup> [General comment No. 25 \(2021\) on children’s rights in relation to the digital environment](#),

Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.15

- Care Leavers; and
- Young People of such description as the Minister (for Children and Families) may specify by Order.

#### FINDING 36



The CYPES Online Safety Policy does not apply to the Children's Residential Service, however, residents are provided with internet usage rules and expectations, and individual care plans and safety strategies are used to manage vulnerabilities and safeguard against online harm. The Panel was informed that Children's Services is undertaking a comprehensive policy review.

#### FINDING 37



The Residential Service uses a system called Sophos to monitor wi-fi use and filter or block harmful content from any device connected to the wi-fi, however, the Panel found that internet filtering software was not in place at the two Children's Short Breaks Homes. It was confirmed in May 2025 that this would be addressed and implemented at those locations in the near future.

#### RECOMMENDATION 17



The Minister for Children and Families should ensure that the updated policies for the Children's Services include clear provisions for online safety, with specific measures to mitigate risks associated with online harm and mobile data access for looked after children who are in the care of the Minister.

## Cybersecurity

The Government of Jersey is developing a draft Cyber Security (Jersey) Law (the 'CSJL') and this has been highlighted to the Panel as one of the ways in which the Digital Economy Programme is supporting the online safety of citizens in Jersey.<sup>183</sup> The Panel asked whether the CSJL would provide protection for individuals from online harms and was advised that it was designed as a resilience law. The Minister for Sustainable Economic Development advised that it *"is designed to be effectively a resilience law, it is about making sure that the Island is secure and prepared against attacks on certain parts of its essential infrastructure"*.<sup>184</sup>

The Minister advised the Panel that the development of the CSJL law had not taken any specific consideration about the protections that the law could provide for more vulnerable citizens and children as it was not part of the intended scope, or original purpose which was focused on Jersey's digital infrastructure. He stated that: *"the Cyber Security Law and what it has been designed for is not the sort of place you would be seeking to put the protection of children from content in."*<sup>185</sup> It was clarified that this was indirectly supporting the online safety of citizens in Jersey by keeping bad actors out of the Island.<sup>186</sup>

The Panel explored whether the CSJL would include any particular standard for cyber security tools in schools, for example firewalls and was advised that the newly established Cyber Security Centre would have the power to set standards, but that it would be down to CYPES how these were implemented. The CSJL serves as a framework that allows for the introduction of secondary legislation alongside the broader cyber security strategy, which could be used to establish minimum standards where necessary.

<sup>183</sup> [Letter – Minister for Sustainable Economic Development – 31<sup>st</sup> March 2025](#)

<sup>184</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.20

<sup>185</sup> [Ibid](#), p.21

<sup>186</sup> [Ibid](#), p.21



The Panel has noted that the Jersey Cyber Security Centre is expected to require increased funding. Its 2025 budget was £1,028,000. This funding supports the Centre's education and monitoring functions. Plans are in place for it to become an independent, grant-funded entity. The Minister for Sustainable Economic Development noted that costs to Jersey would be offset by contracting the Centre to deliver services for Guernsey. The Assistant Minister also remarked that current spending on cyber security is "*shockingly low*" compared to other jurisdictions.<sup>187</sup>



#### FINDING 38

The Cyber Security (Jersey) Law is a resilience law with the purpose of ensuring the safety of the Island's digital infrastructure and providing online safety to citizens as a consequence of this. It is not a law that is designed to provide any protection for children from content on the internet.

### Provision of support

Throughout the review, Ministers emphasised the role of both education and parental involvement in safeguarding children. Support for children [during school time](#) is discussed in the section above and the [role of parents, caregivers and family members](#) are detailed in a later section.

Separately, it must be recognised that protection does not always equate to prevention, therefore, consideration of 'protection' could also involve support mechanisms activated after harm has occurred. The Panel explored what assistance is currently available in such cases.

When asked whether protections exist for children affected by online harm, the Minister for Children and Families, referred to these support mechanisms and advised that:

*Yes, there are protections there for those children that report them. Those can be the police, they can be that they can get help through the Y.E.S. Project and counselling. Those protections are there, so I am not concerned that we have not got protections.*<sup>188</sup>

The Minister for Children and Families also referenced the role of the Children's Mental Health and Wellbeing Services, he explained that they were increasingly integrating digital wellbeing into its support for families and that:

*Further training and support for these staff are being reviewed to be able to consistently provide practical information on issues such as screen time management, identifying signs of digital anxiety or addiction, and understanding cyberbullying. The aim is to ensure that early support services are not only clinically responsive, but also relevant to the challenges children and families face today, particularly in the online space.*<sup>189</sup>

<sup>187</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.24

<sup>188</sup> [Ibid](#), p.34

<sup>189</sup> [Letter – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

## Types of Online Harm

As outlined in an earlier section, the organisation [Internet Matters](#) suggest that it is important to understand *who* is harmed and *how*. The following subsections outline different types of online harm, aiming to offer a high-level overview of the context for children in Jersey.

### Child Sexual Abuse

Children can be protected from online child sexual abuse through a coordinated approach involving technological safeguards, legal frameworks, education, and professional and parental vigilance.

As referenced in the [table](#) shared earlier in this report, there is existing legislation in place that criminalises the possession, distribution, and creation of child sexual abuse material (CSAM), and mandates reporting obligations for professionals.

The NSPCC (National Society for the Prevention of Cruelty to Children) is a leading children's charity fighting to prevent child abuse in the U.K. and the Channel Islands. In a direct submission to the Panel, the NSPCC advised that "*the scale and complexity of online child abuse continues to increase*"<sup>190</sup>. They highlighted that:

*Child abuse is not siloed by country or region, and neither is the online world: online child sexual abuse is a global challenge. At present, the UK, the EU, and many governments across the world are putting in place legislation to protect children from online harm.*<sup>191</sup>

The Internet Watch Foundation (IWF), which is based in the U.K. but accepts reports from across the world, works to end child sexual abuse imagery online. The IWF reports rising volumes of abuse imagery and emphasises that online child sexual exploitation is a worldwide issue.<sup>192</sup> It is understood that the online environment provides easier access to child sexual abuse material for those that want to access it, and environments where there is insufficient action to identify and combat predatory behaviour in online spaces, it can create an increase in harmful practices.<sup>193</sup>

In Jersey, the SPB (Safeguarding Partnership Board) published a multi-agency [strategy on Child Sexual Abuse and Exploitation \(CSAE\)](#) in July 2022, which aims to identify and prevent child sexual abuse and exploitation and help its victims. The SPB's submission to the Panel's review provides details about their public awareness campaign, which is a key objective of the strategy:

*"The campaign isn't technology or app focused to restrict or control children's behaviours in the online world. Instead, it focuses on educating and empowering adults to understand digital risks and feel confident in discussing them with children. By fostering open conversations, children are more likely to share their online experiences, ensuring they can seek help and support when needed and in a timely way".*<sup>194</sup>

---

<sup>190</sup> [Written submission – Online Harms Review - NSPCC Jersey – 21<sup>st</sup> March 2025](#)

<sup>191</sup> [Ibid](#)

<sup>192</sup> <https://www.iwf.org.uk/about-us/> (accessed August 2025)

<sup>193</sup> 'The children's rights-by-design standard for data use by tech companies', P. Hartung, UNICEF, Good Governance of Children's Data project, November 2020, p. 2

<sup>194</sup> [Written Submission – Online Harms Review – The Safeguarding Partnership Board](#)

During the public hearing with the Minister for Justice and Home Affairs and the representatives from the States of Jersey Police, the Panel learned that the [Protection of Children \(Jersey\) Law 1994](#) defines a child as under 16 for the purposes of indecent image offences, whereas most other jurisdictions use under 18 as a standard and the impact of this difference:

***Detective Superintendent, States of Jersey Police:***

*The 1994 legislation for indecent images is only applicable to children and young people under 16, whereas everywhere else it is 18, and the consequence of that, not only from a safeguarding point of view of your older children, is the impact on [Head of Digital Forensics Unit's] digital forensics team, because we cannot use software that they use elsewhere which automatically scans the images and will pick out the ones under 18. So we have to individually look at all these images, which is not only time-consuming, but from an officer well-being point of view, is less than ideal. So I do not know the reason why in 1994 it was 16, there will have been a good reason for that, but in this day and age, every other piece of legislation would identify a young person as under 18, and it has that impact in the workplace for us.<sup>195</sup>*

The interpretation in the legislation provides the definition of “child” as a person under the age of 18 years, however, Article 2A which refers to indecent photographs or pseudo-photographs of children states:

**2A Evidence of age**

*In proceedings under this Law relating to any indecent photograph of a child a person is to be taken as having been a child at any material time if it appears from the evidence as a whole that he or she was then under the age of 16 years.<sup>196</sup>*

The Panel has learned that harmful sexual content which depicts a child can be reported to the IWF under a report function which enables them to assess, remove, and block such content in collaboration with law enforcement and internet service providers in the relevant jurisdiction.

The Panel has noted commentary around the matter of “self-generated” imagery, i.e. where the child has taken sexual pictures of themselves. General Comment No. 25 states that “Self-generated sexual material by children that they possess and / or share with their consent and solely for their own private use should not be criminalised”<sup>197</sup>, however, the Children’s Commissioner has said that this term is potentially misleading and that often the images may be taken under duress or as part of grooming the child.

The Panel is aware that there are planned amendments to Jersey’s Sexual Offences Law to address non-consensual sharing of sexual images and strengthen protections against emerging forms of online sexual harm. The changes will also criminalise possessing, making, sharing, threatening to share, and causing to make or share intimate images or deepfake images without consent. There will also be a new offence to criminalise the sending of unsolicited pornographic intimate images without consent.<sup>198</sup>

---

<sup>195</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.14

<sup>196</sup> [Protection of Children \(Jersey\) Law 1994](#)

<sup>197</sup> [General comment No. 25 \(2021\) on children’s rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.19

<sup>198</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p. 19

As previously referenced, there is a challenge to address the gap that is created by the global nature of the internet and the local scope of legal authority in relation to online harms. Where any perpetrator is overseas, any legal action becomes more complicated and cross-border cooperation is required. In relation to this challenge, the Panel asked questions about the use of VPNs and was advised that:

**Deputy C.D. Curtis:**

*Can I just ask, have you had evidence of what people might be using V.P.N.s for around any criminal activity, do you see that happening?*

**Head of Digital Forensics Unit, States of Jersey Police:**

*Yes, when it comes to C.S.A.M. (Child Sexual Abuse Material) and indecent images, people will use V.P.N.s to mask their identity and mask their location. So while the V.P.N. will say that they are in the United States, but they could be here in St. Helier, we just would not know. They could be anywhere in the world and it will mask both their identity and their location. The providers of those are equally located often overseas and in countries where we probably would not be able to serve any notice on them to then say: "Right, we have this information, they are using your service. Can you then identify that person from that?" We probably would not get any success and any response from that.<sup>199</sup>*

#### FINDING 39



In Jersey, there is legislation that makes the creation or distribution of child sexual abuse material (CSAM) a criminal offence. There is also a multi-agency [strategy on Child Sexual Abuse and Exploitation \(CSAE\)](#) published by the Safeguarding Partnership Board. Where CSAM is found, it can be reported to the Internet Watch Foundation who will work internationally to remove the content from the internet. There are plans to make amendments to the Sexual Offences (Jersey) Law 2018 to address non-consensual sharing of sexual images.



#### RECOMMENDATION 18

The Minister for Children and Families should amend the Protection of Children (Jersey) Law 1994 to ensure consistency in the definition of a child as any person under the age of 18. This revision should apply uniformly throughout the legislation, including provisions relating to indecent photographs, so that protections explicitly extend to all individuals under 18 years of age.

## Exposure to harmful or inappropriate content, including suicide and self-harm

Harmful, inappropriate or unsuitable content covers a wide range of material, for example: sexual abuse material, pornography (when viewed by minors), content that promotes suicide, encourages self-harm or eating disorders, violent content, terrorist content, or hate speech.

In a written submission to the Panel, the Children's Commissioner highlighted the concern that children are frequently exposed to harmful content and there was evidence that this might be more common than many forms of online sexual risk:

*"Children may encounter inappropriate content, including self-harm promotion, and misinformation, graphic violence, adult content, and harmful social pressures (e.g., body image ideals). Evidence from the NSPCC shows that children are more likely to*

<sup>199</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.29-30

*be exposed to harmful content risks than most types of online sexual risks. They also highlight that the evidence consistently shows that at least one in twelve children have experienced harmful content online such as online pornography, content that encourages suicide, self-harm and eating disorders, cyberbullying and hate crime”.<sup>200</sup>*

Various legal and policy protections are described generally in the section about [Legislation](#) above, however, in summary, the Panel understands that Article 51 of the Telecommunications (Jersey) Law 2002 is the most relevant provision of the law in relation to online and internet facilitated harms can be used to address exposure to various inappropriate or unsuitable content online.

Furthermore, whilst there are laws that make it a criminal offence to create or distribute CSAM ([Protection of Children \(Jersey\) Law 1994](#)) or promote terrorist content ([Terrorism \(Jersey\) Law 2002](#)), there is no legislation in Jersey which requires age verification for accessing online content that may be considered harmful to children, for example, adult pornographic content, or content that contains depictions of serious violence.

As referenced in an [earlier section](#), there are safeguarding procedures and digital safety measures such as filtering technologies used in schools. The Head of Governance and Digital for CYPES advised that the tools that were available in education settings were also available across some of Jersey’s children’s homes as well, she explained that:

*There are different types of tools, but they are filtering contents. No tool is infallible; it is probably important to highlight that. But the tools are also adaptable, so once it has been highlighted that that type of image, for example ... because the tools can pick out images as well and block them, and they can identify to an extent deep fakes, not necessarily in its entirety and not always. Again, as technology moves on and it looks more realistic, it is harder for the software to develop, but the software is also always developing.<sup>201</sup>*

In one submission to the Panel, a parent shared various concerns in relation to the use of smartphones in schools, saying that: “Children are regularly shown photos of inappropriate images (it doesn’t matter if the school has these apps barred- they are screen shots) and the child is so effected by them they get so low”.<sup>202</sup>

#### Self-harm and suicide related content

In Jersey the [Homicide \(Jersey\) Law 1986](#) makes it an offence to aide, abet, counsel or procure a person’s suicide. General criminal laws may also apply in some circumstances, for example if a death forms part of a wider pattern of abuse. This type of harm is considered a risk online as individuals could have easy access to information, materials, or forums that discuss and promote suicide or self-harm.

Whilst exposure of children and young people to online material referring to suicide or self-harm would be a serious safeguarding risk, the law does not contain specific offences relating to sharing this type of content generally and any relevant legislation would likely frame protection from these harms within broader safeguarding duties, for example, those provided for in the [Children and Young People \(Jersey\) Law 2022](#) and the [Protection of Children \(Jersey\) Law 1994](#).

As an example, the Children and Young People (Jersey) Law 2022 does not specifically reference inappropriate online content, but it does impose duties on public bodies and

---

<sup>200</sup> [Written Submission – Children’s Commissioner for Jersey](#)

<sup>201</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.35

<sup>202</sup> [Written Submission – Online Harms Review – Anonymous 1](#)



safeguarding partners to ensure the welfare of young people, promote wellbeing and report any concerning behaviour. The law relies on the public bodies and safeguarding partners to interpret their duties in light of emerging risks.

The Panel is aware that the '[Connected in Hope: A Strategy for Suicide Prevention in Jersey 2025 -2029](#)' was published by Public Health Jersey in April 2025. With reference to protective factors the strategy indicates that there are positive aspects to social media, in addition to the potential harm. It says:

*Among the social factors considered to prevent suicide, social media was referenced repeatedly. It was expressed that reducing social media use, particularly among young people, would be beneficial, as would using social media for signposting, and to share resources to promote good mental health.*<sup>203</sup>

Therefore, whilst social media can contribute to the challenges faced by some individuals, it also has the potential to be part of the solution, if used for signposting. The Panel suggests that there could be opportunities for connection between this strategy and the work that the Government may develop in relation to online safety in relation to addressing both suicide and self-harm, for example, connections through the BASC framework.

With regards to legislation, during the public hearing in October 2024 the Panel was advised by the Minister for Sustainable Economic Development that suicide and self-harm protections could all be dealt with by "our laws" but that, at that point in time it was "too early" to say how that would be incorporated into any changes.<sup>204</sup> When the Panel asked the Minister again in May 2025, he advised that there had been no specific work to separate types of harm.<sup>205</sup> The Assistant Minister pointed the Panel to the platforms own terms of use as the first port of call where there were inappropriate posts, for example, that would violate the platform's own guidelines.<sup>206</sup>

In a public hearing in May 2025 the Detective Superintendent, States of Jersey Police informed the Panel that certain jurisdictions, such as Scotland, have successfully pursued prosecutions in cases involving the suicide of a young person. However, it was noted that this remains a "difficult area" for law enforcement.

During the hearing it was confirmed that no specific provisions relating to suicide or self-harm related content online were currently being developed in Jersey. However, the Minister for Justice and Home Affairs suggested that "if we are addressing online safety and we are asking people to take material down, then this would be no different to that, I would suggest."<sup>207</sup>

The Panel's understanding is that there is a key difference between the take down requests that relate to any material that relates to an individual's own personal data information and, separately, general content that may be harmful to an individual that sees it due to factors like their age.

The Panel observes that many online platforms offer 'take down' or 'report' functions, enabling users to flag harmful content. The IWF can work to remove CSAM material, however, suicide and self-harm related content is not in their direct remit. Within the legislative context the

---

<sup>203</sup> '[Connected in Hope: A Strategy for Suicide Prevention in Jersey 2025 -2029](#)', Public Health Jersey, April 2025, p.48

<sup>204</sup> [Transcript - Standalone Hearing re Online Safety for Children in Jersey - 4th October 2024](#), p.13 and 29

<sup>205</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.28

<sup>206</sup> [Ibid](#), p.28

<sup>207</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.20



concept of “take downs” has primarily been discussed in relation to proposed amendments to data protection legislation. The Panel emphasises that this relates to online harm that involves personal data and is unlikely to apply to broader content reporting mechanisms that do not concern the reporting individual’s own personal information.

In respect of suicide and self-harm content, Government officers advised the Panel that it was a challenging area and as it had not been an area of focus as it was not part of a recommendation in the VAWG Taskforce report.<sup>208</sup> However, the VAWG Taskforce Recommendation 10 was “*The Government of Jersey should ensure that similar protections to those afforded by the UK Online Safety Bill, in relation to the regulation of online platforms to ensure they are protecting their users, are brought in through other means*”. It was suggested to the Panel that content related to suicide and self-harm was considered part of the “legal but harmful” concept that was part of earlier drafts of the OSA and was not part of the approved law.

The term “legal but harmful” was originally intended to refer to content that was not illegal, but could be considered harmful to children, for example, pornography or content that does not meet a criminal threshold, but which promotes, encourages, or provides instructions for self-harm or eating disorders. In various evidence, Ministers highlighted to the Panel that the term “legal but harmful” was removed from the OSA as it was considered that it “*would cause considerable legal uncertainty, might lead to over-censorship and be very difficult to enforce*”.<sup>209</sup> The Panel was also advised that there would be a challenge in finding an exemplar of a country that has managed to deal with the concept of “legal but harmful” effectively.<sup>210</sup>

The Panel understands that, despite the removal of the “legal but harmful” aspect of the OSA, it does provide protections regarding suicide related content and self-harm material. The OSA requires regulated platforms to assess and mitigate the risks posed by harmful material, including content that promotes or glorifies suicide or self-harm. It also places a duty on service providers to implement proportionate systems and processes, such as content moderation, user reporting mechanisms, and age-appropriate design features, to reduce children’s exposure to such content and to respond when it is identified.<sup>211</sup>

The update on Recommendation 10 in the [Violence Against Women And Girls: Annual Progress Report](#) (published by the Minister for Justice and Home Affairs on 10<sup>th</sup> June 2025) included the following information which noted that work on the recommendation was “in progress”:

*Based on lessons learnt and best practices, a legislative framework that is proportionate and effective for Jersey is in development. The aim is to empower a person exposed to online harms to effectively request the removal of the harmful content from the platform. Where that does not happen in a timely manner, the respective person should have the right to address a complaint to Jersey Office of the Information Commissioner (JOIC). Discussions are underway with JOIC and the Law Officer’s Department to define which additional enforcement powers JOIC might need to enable them to provide relief for victims faster and more effectively.*<sup>212</sup>

Therefore, whilst the Government of Jersey has previously committed to address all of the VAWG taskforce report recommendations, including a commitment to regulate online

---

<sup>208</sup> [Ibid](#), p.20

<sup>209</sup> [Letter – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

<sup>210</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.21

<sup>211</sup> <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/protecting-people-from-online-suicide-and-self-harm-material> (accessed 27/08/2025)

<sup>212</sup> [Violence Against Women and Girls: Annual Progress Report](#), Government of Jersey, June 2025, p.6

platforms (Recommendation 10), the work is focussing on removal of content that harms an individual, rather than imposing wider requirements to regulate content. The Panel has also established that no work is being progressed to address impose duties for online platforms to mitigate risks posed by harmful content that refers to suicide or self-harm.

Ministers have spoken of the “*umbrella effect*” of the U.K.’s OSA, however, the Panel highlights that this is not thoroughly tested. With regards to age-verification measures the Panel has noted that this to be unsubstantiated, however, we have not undertaken any informal evaluation regarding the potential influence of the umbrella effect on other types of content, as such an inquiry would likely necessitate a more structured and methodologically designed test to account for the various influencing variables.

#### Age verification

The Panel explored the topic of age verification with Ministers in public hearings, as it related to exposure to potentially harmful or inappropriate content. Legal adult content, for example, pornography, may be considered harmful to children due to age-appropriateness and therefore the OSA does not ban the content, but inserts protective measures (such as age-assurance) to prevent minors from viewing it online.

The UNCRC’s General Comment 25 says that: “*Robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements.*”<sup>213</sup>

The Panel referenced the OSA’s introduction of age-verification to access porn sites and asked the Minister for Sustainable Economic Development whether Jersey would introduce comparable legislation. He responded to say that this was not an area that the Government was planning to pursue and suggested that, in relation to online safety, it could offer a false sense of security for parents:

#### ***The Minister for Sustainable Economic Development:***

*At the moment, we have not been looking at that side of it. It is interesting because one of the things with age verification is that is also means you are giving away personal information straightaway and so there is kind of a jumpstart position or even a paradox you could say and, obviously, we recommend to Islanders to give away as little personal information as possible in general. Age verification systems for pornography sites usually require a face picture and a picture of the passport, which is the user’s most private data, and that data could be used for scams and criminal activity, so there are issues around age verification. There is also a social issue, which is that age verification systems create a false sense of security for parents and if you go back many years before the internet, whether it was young people trying to buy alcohol or young people trying to buy magazines on top shelves, there was always young people trying to avoid age verification systems. That is part of growing up and that is the truth of it. Age verification systems might again - coming back to the discussion about parental responsibility - give a false sense of security. There is also the V.P.N. issue. Age verification systems get a V.P.N. They are free and whatever you can get in a couple of clicks so you are immediately pretending you are from a*

---

<sup>213</sup> [General comment No. 25 \(2021\) on children’s rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.19

*country that does not have an age verification system. In short, that is not where we are looking at the moment.*<sup>214</sup>

This scepticism about the robustness of age-verification procedures was echoed by the Minister for Education and Lifelong Learning and he suggested a more community-based approach, with a key role for education, would be appropriate:

*I am sorry, forgive me for being cynical, but I do not think there is such a thing as a robust age verification process in that way. So social media content is ... we have given access to the entire sum total of human knowledge to everybody with a phone in their pocket, good, bad or indifferent. How we control that is a societal discussion that we need to have. Schools can play one role in that.*<sup>215</sup>

The Panel also asked the Minister for Children and Families what role there was for Government with regards to supporting age verification. The Minister advised that the responsibility was firmly with platform owners and providers to provide age verification for certain services. The Minister said:

***The Minister for Children and Families:***

*[...] I mean, governments can put pressure on them in one means or another to do that, but at the end of the day it is the platform owners who have to step up.*<sup>216</sup>

The Panel has explored the role of [digital platforms](#) later in this report, however, notes the concerns raised by Government about the robustness and validity of the age-verification process.

In Jon Tarrant's written submission to the review, he referenced the Minister for Sustainable Economic Development's responses to Panel questions about age verification and opined that:

*The Minister for Sustainable Economic Development is correct in stating current age-verification processes can be circumvented but this is not a reason for inaction. There will probably never be a foolproof method of age-verification, nor of network-level filtering in general, but if we claim to be waiting for such a solution then we will wait for ever. It is better to do something than to do nothing.*<sup>217</sup>

In relation to the consideration of the best interests of the child in the digital environment, a report the report published by the Digital Futures for Children centre has highlighted that "Determining the best interests of a child or children is the obligation of States and cannot be left to technology companies, which, nonetheless, are required to act on such determinations".<sup>218</sup> This obligation for State parties, such as the Government of Jersey, is rooted in the UNCRC Articles which are detailed in an [earlier section](#) of this report.

---

<sup>214</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.27

<sup>215</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.28

<sup>216</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.18-19

<sup>217</sup> [Written Submission – Online Harms Review – Jon Tarrant – 23<sup>rd</sup> May 2025](#)

<sup>218</sup> Sonia Livingstone et al., [The Best Interests of the Child in the Digital Environment](#), Digital Futures for Children Centre, March 2024, p.2

#### **FINDING 40**



There is legislation that makes it illegal to aide, abet, counsel or procure a person's suicide, however, unlike the United Kingdom, Jersey does not have legislation that mandates online platforms or service providers to monitor or remove inappropriate digital content, including suicide related content and self-harm material, or to implement age-assurance measures for accessing certain material and the Panel has established that no work is being progressed to address this.

#### **FINDING 41**



The Panel notes that within the current legislative framework, the concept of "take down requests" has predominantly been considered in the context of proposed amendments to data protection legislation. These measures are intended to tackle online harms involving personal data and are unlikely to apply to wider content reporting mechanisms, especially where the material does not directly concern the personal information of the individual making the report. In such cases, platform-specific guidelines are more likely to govern how the content is handled.

#### **FINDING 42**



The Government of Jersey has committed to implementing all Violence Against Women and Girls Taskforce recommendations, including regulating online platforms (Recommendation 10). However, current efforts by the Government focus solely on removing harmful content targeting individuals, without broader measures to regulate content, which is a significant part of the purpose of the OSA.

#### **FINDING 43**



The Government of Jersey currently has no plans to introduce regulations requiring service providers to implement age-verification measures for users accessing specific online content, such as pornography. Ministers have been critical of age-verification measures. The Minister for Sustainable Economic Development has stated that requirements to provide age verification are not considered appropriate for Jersey citizens, as it involves individuals disclosing highly sensitive personal information to third parties. Additionally, it may create a misleading impression of online safety, given that age-verification measures can be easily circumvented, for instance, using a VPN.



#### **RECOMMENDATION 19**

The Government of Jersey should develop legislation that mandates online platforms and service providers to monitor or remove inappropriate digital content, for example, content that encourages suicide or self-harm.



#### **RECOMMENDATION 20**

The Ministerial Group should seek specific guidance from Public Health in order to create coordination and joint working between the 'Connected in Hope: A strategy for Suicide Prevention in Jersey 2025-2029' and any work that the Government progresses in relation to online safety, for example under the Building a Safer Community framework.



#### **RECOMMENDATION 21**

The Government of Jersey should observe and evaluate age assurance measures introduced by other jurisdictions to determine their effectiveness in protecting children and consider the benefits and risks of adopting similar safeguards locally.

## Online grooming, harassment or stalking

In Jersey there is existing legislation that criminalises online grooming, harassment, or stalking, however, the Panel has learned that there are legislative developments planned in this area in response to the VAWG report recommendation. The existing legislation is:

- The [Sexual Offences \(Jersey\) Law 2018](#): includes articles which address:
  - Sexual grooming of a child, where the recipient of an explicit photograph is under the age of 16 (Article 15 (5));
  - Causing a child to look at an image of any person engaging in a sexual act (Article 14(2)); and
  - Voyeurism, i.e. where the image is taken without the consent of the person photographed (Article 36(3)).
- The [Crime \(Public Order\) \(Jersey\) Law 2024](#): Article 6 addresses harassment, however, this cannot be applied to conduct that occurs only on one occasion, for example, one-off communications sent on social media.
- The [Telecommunications \(Jersey\) Law 2002](#): Article 51 addresses improper use of a telecommunications system.

To try and gauge the scale of these forms of harms, the Panel asked the Minister for Justice and Home Affairs for data about both reported crimes and convictions where the victim was a child. The Minister did provide information to the Panel, but this was provided in confidence as it was noted that low numbers in some of the areas may lead to victim identification.

The Children's Commissioner pointed the Panel to some U.K. based data and said that:

*"The NSPCC in the UK has documented an increase in online grooming cases, emphasizing the need for stronger child protection measures. Over 9,000 child sexual abuse offences involved an online element in 2022/23 and 6,949 sexual grooming offences were recorded by police in the United Kingdom. The research also found that Snapchat and Meta-owned platforms were the platforms most commonly associated with offences of sexual communication with a child".<sup>219</sup>*

During a public hearing with the Minister for Justice and Home Affairs and the States of Jersey Police, the concept of "*stranger danger*" was discussed. It was noted that while traditionally this referred to physical encounters in public spaces, the modern equivalent now exists through digital devices such as smartphones and tablets. This shift presents new challenges, as the threat is often invisible, unlike in physical settings where the individual can be seen:

*... the stranger danger chat before was physicality, whereas now the stranger danger is the iPad, the phone, and that danger is probably worse because that person is not seen necessarily, whereas in an open space, in a stranger danger, the person is seen.<sup>220</sup>*

The unseen dangers of digital communication and modern "*stranger danger*" are particularly pertinent and the Panel suggests that they require attention<sup>221</sup>. A submission to the Panel

---

<sup>219</sup> [Written Submission – Children's Commissioner for Jersey](#)

<sup>220</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.22

<sup>221</sup> **NOTE:** During the factual checking process, it was highlighted to the Panel that Whilst 'online harms' not specifically covered in BASC education programme, it does cover exploitation including online both in States of Jersey Police and Jersey Customs and Immigration Service (JCIS) sessions. The JCIS session covers what data children share and how it may be used but also what a 'stranger' might ask for and how they may use this to exploit a child.



suggested that the Sexual Offences (Jersey) Law 2018 be expanded to include misinterpretation:

*I propose that grooming offences under the Sexual Offences (Jersey) Law 2018 be expanded to include a specific offence of an adult **misrepresenting their age, identity, sexual orientation, sex, or gender to a minor** for the purposes of facilitating communication with that minor.*

*This would:*

- *Reflect the **realities of online grooming**, where deception is often a key tactic.*
- *Target wrongdoers who we can do something about – those living locally/in the "near abroad"*
- *Close a current gap in the law that allows harmful behaviour to go unpunished.*
- *Align with emerging international best practices in child protection.*

*For example, such a law might have given the authorities more tools to confront the behaviour in AG v Snepp [2025]JRC029 – and possibly have given rise to more effective and earlier intervention.<sup>222</sup>*

The Panel understands that per the Sexual Offences (Jersey) Law 2018, misrepresentation can affect the validity of consent, but not all forms of misrepresentation are automatically criminal offences. In the context of digital communications, this could be an area that the Government of Jersey analyses to assess whether expanding offences about misrepresentation could provide further protection for children in Jersey targeted or harmed online by individuals operating within the local area.

From a legal perspective as with various aspects the Panel understands that Article 51 of the Telecommunications (Jersey) Law 2002 is the most applicable provision as it legislates against the improper use of a telecommunications system. During the standalone public hearing in October 2024 the Minister for Justice and Home Affairs explained that one of the challenges with that current law was that it did not provide anonymity in court proceedings:

*I think the thing is, is that there is no ... the unusual thing about the telecoms law, it comes under Article 51, which is improper use of telecommunication systems. It is used as a catchall for these forms of abuse in lieu of a purpose-built framework, which would better reflect any advances in modern technology. So of course this legislation has been used for text messages and obviously was used for abusive phone calls, annoying phone calls, particular stalking-type of offences. As I said, moreover as this offence does not sit with the Sexual Offences Law, as Deputy Morel said, there is no protection of somebody in relation to this case and their anonymity if it went to court. So I think that is the sort of challenges with it, if you like.<sup>223</sup>*

The Panel was further informed that several of the legislative gaps would be addressed through the responses to the VAWG report recommendations, which includes the introduction of intimate image offences, ensuring the law more effectively captures and responds to these types of crimes.

During the same hearing the Minister for Justice and Home Affairs stated that the Telecommunications Law "is not perfect" but encouraged the public to report threatening

---

<sup>222</sup> [Written Submission – Online Harms Review – Anonymous 19](#)

<sup>223</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.26



messages to the States of Jersey Police and advised that reporting helps build a clearer picture of online abuse and supports ongoing efforts to improve laws.

In response to the VAWG report recommendations the Government of Jersey has committed to develop draft legislation to introduce a standalone Stalking and Harassment Law which will include cyberstalking in its scope.<sup>224</sup> In May 2025 the Panel was advised that the legislation to address cyberstalking was in development, but law drafting had not started yet. It was explained that:

*That is patterned, broadly speaking, on the way the U.K. does stalking, which is to say you have harassment, and then within that activity there is stalking. Then within that there is an aggravated offence, which deals with having caused any serious harm or distress or similar. That is a more complicated piece. It is intended to be seamless between physical and online activity. Both the intimate image piece and the stalking piece do affect children because, for instance, in stalking there will be no minimum age at which you can be stalked or harassed. So it could be applied to somebody engaging with a child if the Sexual Offences Law was not appropriate, or it could be applied to somebody sort of in a school environment, with all of the usual protections around the way we treat the criminalisation of children would come along with that, but it would be applicable for the benefit of children.*<sup>225</sup>

The proposed legislation aims to establish a specific offence of stalking, intended to address both physical and cyberstalking behaviours. In a public hearing with the Panel on 25<sup>th</sup> July 2025 the Minister for Justice and Home Affairs confirmed that the first draft was imminently expected, and the Panel understands that the intention is to lodge the draft legislation during the remainder of this electoral term (i.e. before the general election in June 2026).



#### FINDING 44

Cyberstalking will be addressed within the scope of the legislation that is being developed in response to the Violence Against Women and Girls Taskforce Report recommendations and is expected to be lodged within the existing electoral term (to June 2026).



#### RECOMMENDATION 22

The Minister for Justice and Home Affairs should review the Sexual Offences (Jersey) Law 2018 to consider whether expanding offences about misinterpretation could provide additional protection for children in Jersey, for example, to make it specific offence for an adult to misrepresent their age, identity, sexual orientation, sex, or gender to a minor for the purposes of facilitating communication with that minor.

<sup>224</sup> [Violence Against Women and Girls: Annual Progress Report](#), Government of Jersey, June 2025, p.7

<sup>225</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.8-9

## Cyberbullying

Cyberbullying is bullying that takes place through the electronic communication devices like mobile phones, computers, and tablets. It includes actions that intend to embarrass or humiliate and can occur through messages, social media, forums, gaming platforms, and other online spaces. The NSPCC provides some specific examples<sup>226</sup>, including:

- Sending threatening or abusive text messages;
- Creating and sharing embarrassing images or videos;
- Trolling (sending upsetting messages on social networks, chat rooms or online games);
- Excluding children from online games, activities or friendship groups; and
- Shaming someone online.

The [submission to the Panel from Public Health Jersey](#) highlighted statistics from the 2024 JCYPS survey which found that:

- 17% of young people reported being involved in online bullying.
- 49% of those that reported being bullied in the last year engaged in more than five hours screen time the previous day, compared to 34% of those that hadn't been bullied.

Furthermore, data shared by the Children's Commissioner indicated that in the year ending March 2023, the U.K. Office for National Statistics estimated that over a third of children aged 10 to 15 experienced in-person bullying, and nearly one in five faced online bullying, figures that have remained stable since 2019. While most children reported the bullying to a parent or guardian, a significant minority did not tell anyone, particularly in cases of online abuse.<sup>227</sup>

As referenced earlier in this report, the Children's Commissioner also indicated that there was often an overlap between online and offline bullying:

*I think one of the issues that we need to consider when we think about cyberbullying is that cyberbullying tends to be an extension or a reflection of actual in-person bullying that is also going on. It is not something that frequently happens independently of in-person interaction, so it is a multi-layered issue. I do not think it is as straightforward as just looking at the online piece of that.*<sup>228</sup>

Article 51 of the Telecommunications (Jersey) Law 2002 makes the improper use of a telecommunications system an offence. However, it does not establish the same level of responsibility as the U.K.'s Online Safety Act, which has introduced a duty of care to digital platforms that requires them to assess risks and take steps to insert safeguards which will ensure that children do not access harmful and age-inappropriate content such as bullying and online abuse. An example of this would be that users would not be allowed to comment on livestream videos of minors. They also need to provide parents and children the ability to report problems.<sup>229</sup> Jersey has not imposed this duty of care in any legislation and it is unclear whether there will be an "umbrella effect" in terms of platform design.

---

<sup>226</sup> <https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/> (accessed 27/08/2025)

<sup>227</sup> [Written Submission – Online Harms Review – Children's Commissioner for Jersey](#)

<sup>228</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.4

<sup>229</sup> <https://www.gov.uk/government/collections/online-safety-act> (Accessed 27/08/2025)

The Panel received a number of submissions which referred to instances of cyberbullying. Many of these shared concerns about how smartphones impacted children, particularly in schools or peer group environments.<sup>230</sup> One parent shared:

*I can do what I can at home but I am well aware that he will be exposed to all sorts of other content through his peers. While that may be inevitable and we can have open conversations about it, I would love to be able to send my children to school knowing that they are safe from online bullying and concerning content and are free to be children for at least that part of the day.*<sup>231</sup>

The Panel has previously noted the difficult decision parents face over whether to give their child a smartphone, a dilemma that is especially relevant in the context of cyberbullying. A parent of an 11-year-old who was due to start secondary school shared:

*I am concerned about cyber bullying, even not having a phone will probably open him up to mocking at secondary school.*<sup>232</sup>

Some submissions highlighted specific concerns about the behaviour of individuals using digital devices, noting that those targeted often had no control over the situation. One parent referenced their child's experience:

*The constant feeling that you are being videoed at anytime, being so self aware, even in school. Its goes from a safe space to a overstimulated/ anxious space. Everyone is filming everyone at the moment.*<sup>233</sup>

A young person also shared the following in a submission to the Panel:

*My mates made a pact to ignore me on WhatsApp so that I had to join one of the more addictive apps if I wanted to get replies.*<sup>234</sup>

In response to questions about how schools support children who are experiencing cyberbullying, the Minister explained that “Schools have bullying policies but it is not just about policy. It is about schools being aware that when a child is not in a good place and the support is there. Generally there is support within schools around all areas of bullying and I think that is really important.”<sup>235</sup> The Minister said it was about encouraging a culture of openness to talk about issues, involving families as well. He said that for those impacted, “I would really want people to contact schools, talk to safeguarding and let us deal with those issues as they arrive.”<sup>236</sup>

The Panel notes that the [CYPES Counter Bullying Policy](#) is dated March 2019. The policy acknowledges that the nature of bullying is changing and evolving as technology develops. Schools and educational settings are also each required to have their own counter bullying policies, which are reviewed annually.

The Panel inquired whether CYPES had established thresholds or procedures for schools to follow when a child is found with illegal content on their phone. Specifically, they questioned

---

<sup>230</sup> **Note:** At the time of collecting these submissions CYPES had not announced that it would update the school smartphone policy from September 2025

<sup>231</sup> [Written Submission – Online Harms Review – Anonymous 11](#)

<sup>232</sup> [Written Submission – Online Harms Review - Anonymous 16](#)

<sup>233</sup> [Written Submission – Online Harms Review – Anonymous 1](#)

<sup>234</sup> [Written Submission – Online Harms Review - Anonymous 13](#)

<sup>235</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.38

<sup>236</sup> [Ibid](#), p.39

whether such incidents must be reported to the police and if parental consent is required in these cases. The Minister for Education and Lifelong Learning acknowledged this risk:

*What you think is an innocuous thing, well, that is extremely nasty, is illegal. If you take an image of somebody and misuse it, it is illegal. I think that is the piece of work that needs to go on across our society. These are the laws that exist; this is what is illegal in our society.*<sup>237</sup>

The Panel's question stemmed from concern about the fact that, in Jersey, the age of criminal responsibility is 10, raising questions about the potential for children to be criminalised at a young age. In response, the Minister for Education and Lifelong Learning emphasised that criminalising children should not be a means of correcting behaviour. He explained the crucial role schools play in educating and guiding young people, reinforcing that the focus should be on learning and support rather than punishment.<sup>238</sup>

The Minister for Justice and Home Affairs explained that, as part of the Government's commitment under the Violence Against Women and Girls strategy, specifically recommendations 3 and 24, a centralised database is being developed to collect data on technology-facilitated abuse, including cyberbullying, cyberstalking, non-consensual intimate image abuse, online gender-based hate speech, and cyberharassment. The Minister said that gathering this information is essential to inform future action and hold offenders accountable.<sup>239</sup>

#### FINDING 45



Article 51 of the Telecommunications (Jersey) Law 2002 makes the improper use of a telecommunications system an offence. However, it does not establish the same level of responsibility as the U.K.'s Online Safety Act, which places explicit duties on digital platforms, for example, to implement safeguards against harmful content, conduct regular risk assessments, and ensure systems are in place to prevent and respond to behaviours such as cyberbullying, harassment, and online abuse.

#### FINDING 46



The Government of Jersey is developing a centralised database to collect data on technology-facilitated abuse, including cyberbullying, cyberstalking, non-consensual intimate image abuse, online gender-based hate speech, and cyberharassment.



#### RECOMMENDATION 23

The CYPES Counter Bullying Policy should be updated to provide clear guidance for education settings on how to respond to and reduce cyberbullying, including situations that may involve potentially criminal behaviour, while recognising the importance of safeguarding children without unnecessarily criminalising them.

<sup>237</sup> [Ibid](#), p.39

<sup>238</sup> [Ibid](#), p.39

<sup>239</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.25

## Financial Harms

Financial harms are considered a type of online harm because they exploit individuals through deceptive, manipulative, or coercive digital practices that can lead to emotional distress, loss of money, or compromised personal data, for example:

- online scams and fraud;
- sale of illegal goods;
- in-game purchases or gambling like features;
- financial exploitation through grooming or abuse; and
- identity theft.

Children are not exempt from these activities and can be targeted by criminals as they are considered to be more vulnerable. The Children's Commissioner referenced data from the U.K.'s Safer Internet Centre which shows that:

*...exposure to scams is a regular part of life online for young people, with 79% of 8 to 17-year-olds coming across scams online at least once a month, almost half (45%) at least once a week, and 20% seeing scams online every day. The research highlights that the online scams that children most often encounter are fake giveaways, phishing scams, fake websites, online shopping scams, including fake ticket sales, as well as scams in online games.*

*The research also found that almost half of 8 to 17-year-olds (46%) have been scammed online and 9%, including 8-year-olds, have lost money to an online scam before.*<sup>240</sup>

Digital regulator Ofcom has published research that has indicated the potential links between persuasive features and financial harms for children which found that around 6 in 10 children aged 8-17 are spending money online in social or gaming environments.<sup>241</sup>

The U.K.'s OSA has introduced requirements aimed at protecting children from online financial harms, especially harms which arise from manipulative platform design and unsafe digital environments. These include identifying and assessing risks and implementing safety measures, such as age assurance. However, different company approaches to design and jurisdiction mean improvements may not be implemented universally.

In Jersey, fraud is a customary offence and the Panel queried if it would be codified in future but was advised that the existing law can be used for local based prosecutions. The Panel was advised that:

***Detective Superintendent, States of Jersey Police:***

*[...] We can use the fraud to prosecute for online frauds at the moment, it is generally back to the scams, where are they originating from? If you have got a local offender, yes, we will use existing legislation to deal with that because it is like when we are talking at the start, these offences are adaptable to online, offline.*<sup>242</sup>

This evidence reflects a broader issue common to many forms of online harm: the challenge of jurisdiction. When perpetrators operate outside Jersey, pursuing criminal action becomes significantly more difficult. There is also no certainty that the platform design and age verification would be applicable to users in Jersey.

---

<sup>240</sup> [Written Submission – Online Harms Review – Children's Commissioner for Jersey](#)

<sup>241</sup> <https://www.ofcom.org.uk/online-safety/safety-technology/research-into-persuasive-design-features-and-potential-child-financial-harms> (accessed 27/08/2025)

<sup>242</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.22



#### **FINDING 47**

Prosecuting against online financial harms, such as fraud, is challenging when the perpetrator is not in Jersey and is in another jurisdiction as it makes pursuing criminal action more difficult. It is unclear whether internet users in Jersey will benefit from platform design changes in other jurisdictions.



#### **RECOMMENDATION 24**

The Government of Jersey should assess whether internet users in Jersey will benefit from platform design changes introduced in other jurisdictions to meet legal requirements, particularly those aimed at reducing manipulative design features and mitigating exposure to unsafe digital environments.



## Privacy violations

Privacy violations are a serious type of online harm for children because they expose young users to risks they often don't fully understand or have the tools to manage. In the online environment a privacy violation could be:

- excessive data collection by an organisation, without informed consent;
- sharing of data with third parties, such as advertisers;
- platforms using behavioural data to profile or target users with particular content or advertising; and
- lack of transparency about data policies.

There is some evidence that data profiles of children could be built up before they are born through information about pregnancy provided by parents through online behaviours and shared information.<sup>243</sup> Furthermore, there have been publicised investigations into high-profile digital platforms related to privacy violations. For example, Google was fined for breaching the United States Children's Online Privacy Protection Act (COPPA) by illegally collecting data on the viewing habits of children under age 13 on YouTube, without obtaining parental consent.<sup>244</sup>

The UK's OSA's introduction of age-assurance measures has attracted some criticism as this could create a tension between safety and privacy. These concerns were echoed by Ministers in Jersey (see section above about [age verification](#)). The measures that platforms have to put in place under the OSA must confirm a user's age without collecting or storing personal data, unless absolutely necessary.

The Minister for Sustainable Economic Development advised the Panel that due to the [Data Protection \(Jersey\) Law 2018](#) (the 'DPJL 2018') "*Jersey is already among the jurisdictions with a high level of protection or highest level of protection for personal data, including that of children.*"<sup>245</sup>

The Information Commissioner explained that the DPJL 2018 "*is technology neutral*"<sup>246</sup> and that it contained a few provisions that were particularly helpful when safeguarding children from online harms, namely:

- The core principle of lawfulness, fairness and transparency in the processing of data, means that organisations should explain how data is used in an age-appropriate manner, which helps to prevent data misuse;
- Right to erasure, which helps to limit digital footprints; and
- Parental consent (from someone with legal parental responsibility) for information society services, e.g. for gaming or social media where the child is under 13 years of age.<sup>247</sup>

Furthermore, the Jersey Data Protection Authority (JDPA) has powers which can address harms such as tracking, targeting, lack of transparency and unlawful processing of personal information, but it is not able to address harms related to illegal content or cyber bullying.<sup>248</sup>

---

<sup>243</sup> <https://mitpress.mit.edu/9780262044714/child-data-citizen/> (accessed August 2025)

<sup>244</sup> <https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law> (accessed August 2025)

<sup>245</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.10

<sup>246</sup> [Transcript – Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.2

<sup>247</sup> [Ibid](#), p.6

<sup>248</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

The Panel has learned about the work of the Jersey Office of the Information Commissioner ('JOIC') to educate the public and was advised that:

*In 2024 we engaged with 26% of the total population of Jersey's under 18-year-olds across 18 different schools, with 86% of the young people we engaged with saying that their 'knowledge of JOIC, protection of their personal information and understanding their personal information rights improved as a result of participating in one of our outreach sessions'.<sup>249</sup>*

In Jersey, the age of consent for sharing data in the context of information society service is age-13 but does not extend to all areas of the data protection law.<sup>250</sup> The Children's Commissioner explained that the age of digital consent is primarily linked to data protection legislation rather than an assessment of a child's maturity or educational understanding:

*There has been work undertaken by Click Safe on behalf of the European Union on the minimum age requirements for social media, and it is largely that those platforms tie into what a jurisdiction's minimum age of data protection, data sharing is. It is not an assessment of children's ability at all. It is not an educational assessment at all. It is just related to another piece of legislation which is data protection. Even where laws have been introduced in countries to say 13, that is it, 16, that is it, they have not proven to be particularly effective because the platforms simply find legal ways around them. That is what happens, they find legal ways around them. So the age is quite, I think ... in some ways, it is linked to something that is not necessarily the best measure for online safety, I think that is the answer. I think as with all age limits, it is very difficult to pick one because it always appears arbitrary. You know, it always does appear arbitrary and yet at the same time I think we do need to consider, you know, a legal age because if not then everything is just open to everybody.<sup>251</sup>*

This highlights a significant disconnection between the age thresholds set by platforms and may suggest that reliance on age-based regulation is not a sufficient tool for protecting children online.

#### Limitations of the current law in relation to online safety

The DPJL 2018 and the [Data Protection Authority \(Jersey\) Law 2018](#) ('DPAJL 2018') provides protection from the misuse of individuals data, aligning broadly with the principles of the E.U.'s General Data Protection Regulation ('GDPR'). The laws establish rights for data subjects, duties for data controllers and processors, and enforcement powers for the Jersey Office of the Information Commissioner, however, they do not include a broad regulatory framework as is provided through the DSA or the OSA.

In a written submission to the review from the JOIC it was explained that the DPJL 2018 was limited in how it can address person-to-person online harm or harmful user behaviour not mediated through a controller's own processing systems. This approach is consistent with

---

<sup>249</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>250</sup> [Transcript –Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.10

<sup>251</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.18

other jurisdictions, including the U.K.<sup>252</sup> The submission emphasised that Jersey's data protection laws were not designed as online safety legislation:

*It is important to recognise that neither the DPJL 2018 or DPAJL 2018 were brought into being with online harms in mind and are not “online safety” laws per se and **were not designed to be full spectrum online safety laws**. Whilst the JDPA’s powers under the DPAJL 2018 are increasingly relevant to online harms where such harms involve the misuse or mishandling of personal data by data controllers/processors, it is very important to acknowledge that Jersey’s data protection framework was not designed to operate as a comprehensive online safety regime akin to those that have emerged only very recently in much larger jurisdictions (e.g. the UK’s Online Safety Act 2023 (UK OSA) or Australia’s Online Safety Act 2021 (Aus OSA)) and **it does not have explicit powers to regulate harmful or illegal content, addictive platform design or deal with misinformation/harmful content uploaded by individual platform users**.*<sup>253</sup>

Data protection laws are designed to govern the handling of personal data by entities that determine how and why that data is processed, known as data controllers. The laws focus on ensuring privacy, transparency, and accountability in data use, not on regulating general online behaviour or content. The Panel was advised that the “domestic purposes exemption”<sup>254</sup> meant that the law would not apply to individuals who process data in a personal or household context. It was explained that:

*...in the vast majority of circumstances, an individual will not be considered a data controller or a data processor for the purposes of the law. It certainly does not extend to the processing of personal data in a purely household context, when dealing with just a household activity, which in the main would include personal web browsing and posting on social media. Because of that, our powers and our remit do not extend to cover peer-to-peer image sharing.*<sup>255</sup>

In a public hearing, the Assistant Minister for Sustainable Economic Development also explained the limitations of the DPJL 2018:

*We are very conscious that the Data Protection Law extends to what we call data controllers, and these will tend to be organisations and businesses, and individuals themselves are not subject to that law. We have been looking into the possibility of extending or amending that law to try to create greater protection, but on legal advice and having looked more closely into this, we have come to the conclusion that we are best to proceed with a separate law and it would not be as hefty a law as we have in the U.K. (United Kingdom) in terms of the Online Safety Act, and there is plenty of reasons why we would not wish to replicate that here and why it would not be appropriate.*<sup>256</sup>

The Information Commissioner also verified the information provided by the Assistant Minister about the discussions

---

<sup>252</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>253</sup> [Ibid](#) [emphasis added]

<sup>254</sup> [Ibid](#)

<sup>255</sup> [Transcript – Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.8

<sup>256</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.2-3

*We have had a number of detailed discussions about the limitations with the Digital Economy team at Government explaining how the law is applied and its limitations in respect of taking enforcement action in particular against individuals who are not data controllers and therefore fall outside the scope of the law as it stands, and also how that mirrors the framework set by the General Data Protection Regulation in Europe. I think to expand data protection legislation to cover processing of information by individuals in a private capacity would be novel territory, and I am not sure ... I am certainly not aware of any piece of data protection legislation that strays into that area elsewhere.*<sup>257</sup>

The Panel understands that extending data protection laws beyond data controllers would blur their legal purpose and create enforcement challenges, for example:

- Individual users who post harmful content online are generally not considered to be processing personal data (as per the DPAJL 2018). As referenced by the Assistant Minister, this option was explored but rejected by Government;
- Content regulation would likely require a different legal framework focussed on platform responsibility, not just data privacy; and
- Data protection authorities typically oversee organisations, and do not ‘police’ individual users or moderate content on platforms, therefore enforcement might be a challenge.

#### Proposed legislative change

The Panel noted that in response to queries about online harms Ministers have referenced work underway in the sphere of data protection. In a written response from the Minister for Sustainable Economic Development, he advised that, with regards to protection of personal data: “*We are looking at ways of using this legislative framework to better exercise the rights of data subjects, including those of children, providing further protection in an increasing digital world*”.<sup>258</sup> The Minister expanded on this point in a public hearing, explaining that any changes had to be proportionate for Jersey and that:

*Importantly, Data Protection Laws are based on the consensus of the person whose data is getting processed and so data controllers or processors cannot operate with a person’s data beyond the purpose that they consented to. That is really important in situations where a young person is exposed to forms of pressure that are exerted online, but also where the threshold for legal prosecution has not been passed or where the perpetrator remains anonymous, so we need to bear that in mind as we develop this law as well.*<sup>259</sup>

However, the Panel is concerned that a focus on data protection, which will not include information shared by individuals in a personal capacity, will not cover the scope and full spectrum of online harms.



#### **FINDING 48**

Minimum age requirements for information society services (e.g. social media platforms) are primarily derived from data protection legislation, rather than assessments of children's developmental readiness or online safety needs.

<sup>257</sup> [Transcript – Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.9

<sup>258</sup> [Letter – Minister for Sustainable Economic Development – 31<sup>st</sup> March 2025](#)

<sup>259</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.10

#### FINDING 49



The Government of Jersey has indicated that it will develop legislation to further extend the rights of data subjects, including children. However, in order to remain aligned with the EU's GDPR legislation it will not extend to individuals acting in a personal or household capacity, due to the domestic purpose exemption. As a result, data protection legislation will not adequately address the full spectrum of online harms, particularly those arising from personal content sharing or harmful behaviour between individuals online.

### Misinformation

There is no legislation making “misinformation” or “disinformation” an offence in Jersey and the Panel has heard about the challenges of defining this and balancing it alongside the protection of freedom of speech. Misinformation in online spaces can be a harm for children because they may be less likely to evaluate and question the sources of information, in the long term it can miseducate and manipulate opinions.<sup>260</sup>

Where children engage with particular content, it might be likely that they will see more of the same or related content due to platform algorithms impacting the information they receive, for example, promotion of content related to violence, suicide, radicalisation, or incel culture. However, there is very little published information about how algorithms work and so it is difficult to assess the extent to which these systems may reinforce exposure to potentially harmful or inappropriate material, particularly in ways that affect children's wellbeing or decision-making online.

During the hearing in October 2024, the Minister for Sustainable Economic Development emphasised that:

*There are responsibilities with our freedom of speech, and I will always ... because I believe the need for freedom of speech in a free and democratic society but I absolutely truly believe that you have to balance that responsibility. The laws will show what those responsibilities are.*<sup>261</sup>

This was reiterated in the May hearing with the Minister. The challenge of defining “misinformation” was discussed and he confirmed that there was no work underway on this aspect of harm. The Minister also opined that it was vital to ensure the separation of fact and opinion:

*I am a liberal person, I do believe in freedom of speech and I do believe that we should have the freedom of the individual to choose things. When you accept those as important parts of society, it becomes really difficult to approach the misinformation question. As you were talking, I was just thinking from an atheist perspective, god is misinformation. From a religious person's perspective, god is a truth, do you know what I mean, so that just highlights how difficult it is.*<sup>262</sup>

---

<sup>260</sup> **Note:** During the factual checking process Government officers highlighted that there was some legislative basis for addressing harmful digital manipulation and cited that the Computer Misuse (Jersey) Law 1995 makes it an offence to intentionally modify computer material without authorisation, and the Children and Young People (Jersey) Law 2022 provides statutory duties to safeguard children from harm.

<sup>261</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.30

<sup>262</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.29



One of the criticisms of the U.K.'s draft OSA was around the definition of “*legal but harmful*” content and, therefore, the term was removed from the final draft of the legislation. The Select Committee [i.e. the House of Commons’ Science, Innovation and Technology Committee] report ‘[Social media, misinformation and harmful algorithms](#)’, has explored the technological aspects of online services and markets that can lead to the amplification of false, unfounded or harmful information. This was a follow up to its review of the spread of misinformation following the attacks in Southport, U.K. in July 2024. The Select Committee found that:

*The Online Safety Act will lead to some improvements, but is designed only to protect users from harm that is illegal or affects children. The decision not to include measures related to the algorithmic amplification of “legal but harmful” content, such as misinformation, means that full enforcement of the Act would have made little difference to the online environment that helped to incite the violence of last summer.*<sup>263</sup>

The report also found that “*The broad scale—and serious impact—of misinformation online requires greater transparency and accountability from the government.*”<sup>264</sup> In light of this and in line with the proposed principle of ‘public safety’ the Select Committee recommended that the U.K. government should take further action, specifically, by submitting an annual report to Parliament on the state of misinformation online, tracking trends and issues from the year, and setting out successes and failures in addressing them.<sup>265</sup>

It is worth noting that the Select Committee’s report identified five key principles which they stated were “*crucial for regulation of social media and related technologies*”, namely:

- 1) Public safety: Algorithmically accelerated misinformation is a danger that companies and government need to address—the government and platform companies should work together to protect the public from it.*
- 2) Free and safe expression: Neither government nor private companies should be arbiters of truth. Steps to tackle amplified misinformation should be in line with the fundamental right of free expression, with restrictions where proportionate and necessary to protect national security, public safety, health, or to prevent disorder and crime.*
- 3) Responsibility: Users should be held liable for what they post online, but the platforms they post on are also responsible, especially with regard to the systems used to moderate, circulate or amplify content.*
- 4) Control: Users should have control over both their personal data and what they see online. This includes the right to delete the data stored by platforms and services which is used to drive content and advertisement recommendation algorithms.*
- 5) Transparency: The technology used by platform companies, including social media algorithms, has huge public safety implications, and should be transparent and accessible to public authorities.*<sup>266</sup>

---

<sup>263</sup> ‘[Social media, misinformation and harmful algorithms](#)’, Science, Innovation and Technology Committee, House of Commons, 11<sup>th</sup> July 2025

<sup>264</sup> [Ibid](#)

<sup>265</sup> [Ibid](#)

<sup>266</sup> [Ibid](#)



These principles reflect a recognition of the potential risks associated with “*algorithmically amplified misinformation*” and the use of personal data within social media environments. Larger jurisdictions face challenges in working with digital platforms, therefore, Jersey should consider its own unique challenges due to its smaller scale and jurisdictional limitations. These factors suggest the importance of evaluating how such principles might be adapted to Jersey’s context, rather than overlooking the relevance of the issue of addressing misinformation as a distinct type of online harm.

#### FINDING 50



The impact of false or misleading content, particularly when amplified by algorithms, has been found to be a risk to public safety in the U.K. In Jersey, the Minister for Sustainable Economic Development has confirmed that there are no government plans to introduce specific measures aimed at tackling misinformation online.



#### RECOMMENDATION 25

The Ministerial and Officer groups tasked with reviewing the online safety policy should give due consideration to the issue of algorithmically accelerated misinformation and assess whether, and in what manner, the Government of Jersey intends to respond to this in a local context. As larger jurisdictions have acknowledged, the amplification of false or misleading content through algorithmic systems can pose a risk to public safety, or wellbeing

### Harm to individual health

Just as laws regulating alcohol and tobacco were introduced to protect public health, particularly shielding young people from addictive and harmful substances, it could be argued that online safety legislation would serve a similar protective function in the digital age.

Jersey has laws which prevent the sale of certain products to minors, namely:

- Protection of Children (Restriction on Supply of Goods) (Jersey) Law 2009
- Restriction on Smoking (Cigarettes to Children) (Amendment No. 2) (Jersey) Regulations 2006;
- Restriction on Smoking (Vending Machine) Jersey Regulations 2006; and
- The Licencing (Jersey) Law 1974.

The Panel explored this parallel in a public hearing:

#### **Deputy C.D. Curtis:**

*Seeing as this is concerning children, we have got some examples where children are protected by legislation, for example, from exposure to harm through tobacco, alcohol and so on, so do you think that protecting children from exposure to harm through the conduit of the internet is different from exposure to these other types of harm?*

#### **Assistant Minister for Children and Families:**

*I think it is harder to control, is it not? You can only get alcohol or tobacco from certain places, whereas virtually everybody has access to the internet in one form or another. That is why it is about that education piece and it is about teaching people how to use the internet safely and what to do when it goes wrong and who to alert when it goes wrong, and also to identify what going wrong looks like, because so many people who operate on the internet, they are very devious in the way that they work and lure children and young people into activities that they do not even realise necessarily are*

*harmful. By the time they do realise it is harmful, they are already so far into it they do not know who to turn to.*<sup>267</sup>

The existing legislation which prohibits the sale of certain products to minors reflects a longstanding public health approach to safeguarding young people from harmful consumption. The Panel suggests that the Government of Jersey should analyse the applicability of this approach to digital environments, by examining how online platforms may facilitate addictive or harmful behaviours among children.

There is a step of separation between “screen time” and “online harms” but there is increasing evidence and research to explore links between the two and whether prolonged screentime is a contributory factor to certain types of online harm and is a standalone harm to an individual’s health. In relation to the link to online harms, it is suggested that digital platform design and lack of safeguards can amplify risks of children spending longer amounts of time on devices, therefore, they might be more likely to be exposed to risks or a type of harm.

UNCRC General Comment No. 25 highlights that State parties should proactively respond to emerging public health evidence to protect children’s mental and physical wellbeing:

*States parties should regulate against known harms and proactively consider emerging research and evidence in the public health sector, to prevent the spread of misinformation and materials and services that may damage children’s mental or physical health. Measures may also be needed to prevent unhealthy engagement in digital games or social media, such as regulating against digital design that undermines children’s development and rights.*<sup>268</sup>

Some of the risks of screen time named in the Public Health Jersey submission are obesity, myopia, sleep disruption, mental health concerns, screen addiction and cyberbullying.<sup>269</sup>

In the submission to the Panel from Dr. Chris Edmond, the research that was shared from the Health Professionals for Safer Screens group<sup>270</sup> indicated that:

- A measurement of 2,232 five-year-old children showed that having more than two hours per day of screen time was significantly associated with ADHD behaviours;
- Excessive smart device usage is linked to the high rates of myopia and astigmatism in children; and
- A large longitudinal study of 9- to 14-year-olds found that increased total screen time, social media use, and problematic screen use were associated with a higher prevalence of eating disorder symptoms in early adolescence.

Submissions from members of the public also relayed these concerns about screen time and smartphone use and the dangers of addictive behaviours. One 16-year-old advised the Panel:

*They [States Members] were talking about our "right to be on phones" like that is some kind of freedom. I think it's mental adults think like that, it made me laugh actually, seriously? - we're on our phones cause our mates are, and cause we feel pressure to know what's going on, and because they are ADDICTIVE and we get stuck into doom*

---

<sup>267</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.5

<sup>268</sup> [General comment No. 25 \(2021\) on children’s rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.16

<sup>269</sup> [Written Submission – Online Harms Review – Public Health Jersey](#)

<sup>270</sup> [Written Submission – Online Harms Review – Dr. Chris Edmond](#) p. 7 and p. 9

*scrolling. They might be fun, but it's really hard to put it down, and especially when everyone else is addicted to.*<sup>271</sup>[sic]

The UNCRC's General Comment No. 25 also says that State parties should develop guidance for children, parents, caregivers and educators regarding the importance of a healthy balance of digital and non-digital activities and sufficient rest.<sup>272</sup>

The submission from Public Health Jersey indicated that *"The [2024 JCYPS] survey also highlighted that, when asked their main sources of information about sex, online pornography was more common among males (15%) than females (2%). A study by Lin et al. (2020) found that early exposure to sexually explicit media during adolescence was associated with a higher likelihood of engaging in risky sexual behaviours in emerging adulthood."*<sup>273</sup>

Through the submissions from [Public Health](#), [Dr. Chris Edmond](#), and the [Smartphone Free Childhood Jersey parent group](#), the Panel has been made aware of additional studies and evidence into the use of screens and impact of digital harms. The Panel has not had the capacity to consider and evaluate all of this significant research in detail, but we believe it highlights a need for Government to take a position and potentially intervene on this issue.

#### FINDING 51



State parties should proactively consider emerging research and evidence from the public health sector to help prevent the spread of misinformation, as well as materials and services that may harm children's mental or physical health. Such action would support the Government's obligations under the United Nations Convention on the Rights of the Child (UNCRC).



#### RECOMMENDATION 26: Key Recommendation

The Minister for Children and Families and Minister for Education and Lifelong Learning should engage with Public Health Jersey to explore how evidence-based guidance on screen time can be incorporated into government policy and translated into updated practical measures within education and children's services.

<sup>271</sup> [Written Submission – Online Harms Review – Anonymous 13](#)

<sup>272</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.16

<sup>273</sup> [Written Submission – Online Harms Review – Public Health Jersey](#)

## **Who is responsible for prevention and protection of children from online harms?**

The short answer to this question is: everyone.

The Panel has heard evidence about the importance of a societal approach to tackling online harms. Ideally, this requires action to be taken by a range of stakeholders, including government, technology companies, digital platforms, parents, educators, charities, and international organisations, each of whom has an important role to play.

However, a key challenge in addressing online harms lies in defining the appropriate scope of the societal response, i.e. whether it should be coordinated on an international level or tailored specifically to the context of Jersey.

A submission from Smartphone Free Jersey indicated a central issue relating to online harms:

*When we first started giving smartphones to children, we didn't understand their impact. Over the last few years, smart device technology has evolved at a terrifying speed and the content too easily accessible by children and young people is absolutely horrendous, as are the addictive apps and algorithms embedded into the design of these devices.*<sup>274</sup>

Although this submission centres on smartphones, it shows a broader concern, i.e. the significant lag between technological innovation and the implementation of effective safeguards to mitigate potential harms, this often needs more than a local response.

Further evidence presented by the NSPCC reinforced the importance of global cooperation, stating:

*The best way to protect children is through globally aligned regulation which puts the responsibility upon tech companies to make children's online safety a priority. International harmony in regulation will help keep all children safer, raise standards globally, and show that we can be ambitious when talking about child safety online.*<sup>275</sup>

This evidence highlights the need to consider cross-border regulatory frameworks when shaping local policy. However, as the Panel previously noted, the nature of protection from harm depends on who is affected and in what way. In hearings with Ministers, where specific scenarios were explored, they emphasised the importance of a societal approach rooted in local context.

In response to questions about addressing issues like self-harm and suicide related content the Minister for Education and Lifelong Learning advised that Panel that it was important for different groups to work together to address it. He said:

*I think those groups across our society working together is one of the key things. We cannot do everything in schools. Parents cannot do everything on their own. Young people cannot do everything on their own, they are going to meet a problem where they need help.*<sup>276</sup>

---

<sup>274</sup> [Written Submission – Online Harms Review - Smartphone Free Childhood Jersey](#)

<sup>275</sup> [Written Submission – Online Harms Review – NSPCC Jersey](#)

<sup>276</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.41

Following questions in a public hearing which explored whether protections against online harms differ from those addressing issues such as alcohol or tobacco, the Minister for Justice and Home Affairs acknowledged that online harms present unique challenges, because they are not necessarily seen. She emphasised the importance of fostering community awareness, highlighting the need for individuals to remain vigilant about the behaviour of others in digital spaces. The Minister said:

*That is why it is a job for us all. It is a job for us all, as members of the community, to try to deal with and prevent this as much as we possibly can. So all of us, for me, it is an Island, it is a community thing. So it is about anyone that sees a change in a child, whether that is in school, in the home, in the youth centre, it is about picking up on changes in children and young people, is it not? It would be the same for an adult. You see a change in somebody, you think, what is going on? That is about us all being aligned to what is going on in people's lives, in particular young people, and being able to identify that and think there is something not quite right here.*<sup>277</sup>

While there is broad agreement that safeguarding children from online harms demands a collective societal effort, the following sections will examine the specific roles and responsibilities of various stakeholder groups involved.

## Parents, caregivers and family members

Families are central to providing protections for children from online harms for a number of reasons. They not only reinforce the rules and policies established by wider institutions such as schools and government but also model safe and responsible digital behaviour in everyday life.

As one example, the Minister for Education and Lifelong Learning emphasised the importance of parents and families supporting school policies in relation to mobile phone use:

*Well, it is a challenge, because schools have never bought a child a mobile phone, I believe. I do not think we have ever had a child bought a mobile phone, and, also, we cannot tell parents how to parent, and we do not want the blame game. It is not about blaming parents, it is not about blaming schools, it is about that relationship together to say: "Look, these are real online harms that we need to be extremely careful for our young people. How are we going to do this?" We need the schools' policies to be supported by everybody. So when a school says: "We will not have mobile phones", then the children either do not bring them, but many parents might say: "They are getting the bus home, they are walking home. I want them to be able to contact me."*<sup>278</sup>

This shared responsibility between schools and families is further complicated by the difficult choices parents face, as highlighted in several submissions to the Panel. In the evidence provided to the Panel's review by Smartphone Free Childhood Jersey, they shared that:

*As parents, we are in an impossible position: either we give our children a smartphone, with all the known harms; or we protect them from those harms by not giving them a smartphone, but risk isolating them from their peers at a crucial time in their development. However, even when parents choose to not give their children a*

---

<sup>277</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.35

<sup>278</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.27

*smartphone, once on school grounds, they are not protected from seeing inappropriate content on someone else's smartphone in the playground.*<sup>279</sup>

This shows how parents associate smartphone use with online risks, creating a dilemma: how to shield their children from harm while still letting them engage in the digital world that's so central to their social lives. Their submission also highlights that:

*It's not good enough to say "it's just the parent's problem": parental controls on smart devices are easily bypassed (47% of teens say they have bypassed controls, Parentkind survey 2024) by using VPN software, performing factory resets, or hacking the wifi router.*<sup>280</sup>

In a public hearing with the Minister and Assistant Minister for Sustainable Economic Development, research undertaken by the charity [Internet Matters](#) was highlighted, and the Ministers quoted the statistic that two-thirds of parents had not used parental controls on their child's device.

The Assistant Minister noted that it is parents who buy or provide their children with a device in the first place and raised the point that: *"I believe part of the conversation has to be how well are parents supervising in this respect?"*<sup>281</sup> She explained:

*I think that the easiest way to explain that is children are using devices that, as I have pointed out, their parents have allowed them to have access to or to use. Those devices are capable of being hacked by bad actors and so we have to educate, I think the parents in providing safe devices and safe systems.*<sup>282</sup>

The Minister for Sustainable Economic Development also referenced this:

*There is definitely an element of individual responsibility. When I say individual responsibility, in the case of children, certainly under the age of 13 or 14, that is definitely extended to parental responsibility. Deputy Scott, just earlier, I take the numbers that there were, it said that two-thirds of internet devices, it was found parental controls have not been implemented by the parents. That is down to education and, as I said, but we know that there is a large amount of education going on. Obviously that education is primarily I believe to the children themselves. So there might be a role to more directly interact with parents, but there has to be an acceptance that Government cannot go into people's individual devices and should not and that, where children are concerned, the parents need to educate their own children, put on the appropriate parental controls, because if you have those appropriate parental controls in place, your children should not be seeing pornography on their phones.*<sup>283</sup>

This aspect of parental supervision was explored in public hearings with other Ministers. In response to questions about the Government's role in safeguarding children from online harms, the Minister for Children and Families emphasised that Government must be *"there at the top of the tree"*<sup>284</sup> in ensuring protection. However, he also highlighted the critical need to

---

<sup>279</sup> [Written Submission – Online Harms Review - Smartphone Free Childhood Jersey](#)

<sup>280</sup> [Ibid](#)

<sup>281</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.5

<sup>282</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.19

<sup>283</sup> [Ibid](#), p.13

<sup>284</sup> [Transcript – Online Harms Review Public Hearing - Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.7



provide parents with support and information to help them shield their children, alongside direct education for children themselves. He acknowledged that:

*There is a certain element of parents at home that will have a responsibility for monitoring what their children are looking at. The Government can assist them in that, but they are ultimately the people who are there with their children.*<sup>285</sup>

However, the Children's Commissioner referenced the challenges that parents face in understanding their child's online experience. In a written submission she shared that the IWF statistics from 2023 detailed that 36% of parents are not certain where to turn should they need support or resources when it comes to online safety.<sup>286</sup> This discussion was expanded with the Children's Commissioner in a public hearing:

*[...] it is quite possible for many, many children to say: "This is what I am looking at, here is my device." But unless parents know how to look behind what is on the screen, it is very difficult for them to actually know what their child is looking at or experiencing. So I think digital literacy for parents is frightening, but absolutely essential in addressing online harms. I think one of the key skills in this that none of us, I think, were born with is how to actually talk to your child, how to talk to children about their online world, about their online life. I am not sure that that necessarily rests with education or certainly not solely rests with education. I think that is a much broader initiative that needs to be looked at as to where parents are, how they want to receive this, who is best placed to deliver it, what kind of training is actually needed. But this is about - and I think we need to stress this - digital literacy. It is not about being digitally adept. Many, many children are profoundly digitally adept, but that does not mean that they are digitally literate.*<sup>287</sup>

One written submission to the Panel from a mental health practitioner referenced the expectation placed on parents to have the relevant skills and knowledge to manage their child's online access and suggested that it was unreasonable to expect this:

*The families I work with seek support for difficult or conflictual relationships with their children. For most of these families, unregulated social media / online access significantly compounds their problems, particularly if their children are neuro divergent.*

*The lack of meaningful regulation of social media, and access to online content and games means the whole responsibility for managing and mediating their child's access to the internet has to be managed by parents. Typical protections offered on devices are easy for children to work around.*

*Most of these parents are trying their best to put in place positive, reasonable boundaries around their child's use of devices and access to content. They work hard to find the balance between limiting access and allowing some use to ensure their child or young person can 'play' and socialise online and not be excluded from social networking with friends. This is crucial, as much physical outdoor social activity is planned via online networks.*

---

<sup>285</sup> [Transcript – Online Harms Review Public Hearing - Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.30

<sup>286</sup> [Written Submission – Children's Commissioner for Jersey](#)

<sup>287</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.17

*We expect parents, who are often not digital natives, to have the knowledge and skill to take on the might of the digital / social media / gaming industry to protect their children. It's neither feasible nor fair. It creates significant conflict and stress, and further down the line, contributes to mental health issues and family dysfunction.*<sup>288</sup>

This submission highlights the significant burden placed on parents, particularly when they lack the necessary knowledge or skills to effectively manage their children's online activity. Emma Martins' submission to the Panel reinforced how overwhelming this responsibility can be, underscoring the urgent need for enabling measures to help families navigate the challenges:

*The submissions from parents highlight how desperate they are for leadership, support, and action. There is much talk of the need for parents to step up and take responsibility, but they cannot do so without broader support. Parents are completely over-faced. Rather than look to blame them, let's try and come together as a community to help empower them and protect children.*<sup>289</sup>

The Panel asked Ministers what they would say in response to parents who said, "*I need more help to protect my child from accessing certain content on the internet*", their responses are summarised below:

- **The Minister for Children and Families:** acknowledged that the issue could be "*overwhelming*" in some cases, but highlighted ongoing efforts to enhance parental education, including collaboration with organisations like the NSPCC that offer valuable resources.<sup>290</sup>
- **The Assistant Minister for Children and Families:** stressed the importance of equipping parents and guardians with practical tools, recognising the challenges they face.<sup>291</sup>
- **The Minister for Education and Lifelong Learning:** encouraged open dialogue between parents and schools, suggesting that stronger relationships and shared educational efforts can make addressing online safety more effective.<sup>292</sup>
- **The Minister for Justice and Home Affairs:** said that protecting children from online harms requires a cultural shift, supported by education that clearly defines acceptable online behaviour for both adults and children.<sup>293</sup>

In a report titled '[The children's rights-by-design standard for data use by tech companies](#)', compiled for a UNICEF think tank, it is suggested that:

*...the centrality of parental consent as the only threshold for assessing child protection in the digital environment could imply a mitigation of the responsibility of companies to ensure safe environments for children, free from violations of their rights.*<sup>294</sup>

---

<sup>288</sup> [Submission – Online Harms Review – Anonymous 15](#)

<sup>289</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>290</sup> [Transcript – Online Harms Review Public Hearing - Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.41

<sup>291</sup> [Ibid](#), p.41

<sup>292</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.29

<sup>293</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.34

<sup>294</sup> '[The children's rights-by-design standard for data use by tech companies](#)', P. Hartung, UNICEF, Good Governance of Children's Data project, November 2020, p. 1

The paper advocates a children's rights-by-design (CRbD) standard for use of data by tech companies, it explains that a CRbD approach "*would include the design, development and execution of online services or products used by children, in accordance with the CRC [Convention on the Rights of the Child] provisions and the primary consideration of children's best interests*".<sup>295</sup> This CRbD approach is explored further in the next [section](#) of this report.

The evidence collected by the Panel often referenced the importance of community wide support for parents and caregivers in protecting children from online harms. During the public hearing with the Minister for Children and Families, the resources available on the "[Keeping your child safe online](#)" page on gov.je were specified. It was suggested that these materials would be further developed, and additional support for parents through schools was also highlighted.<sup>296</sup>

In addition to support for parents, the UNCRC's [General Comment No. 25](#) highlights that "*some children reported wanting more support and encouragement in their digital activities, especially where they perceived parents' and caregivers' approach to be punitive, overly restrictive or not adjusted to their evolving capacities*".<sup>297</sup> This suggests that supporting parents in maintaining an appropriate balance could help support children have a positive experience in the digital environment, rather than solely prohibiting their use. Further commentary about resources available for parents and digital literacy is detailed in the section '[Define expectations for digital skills](#)'.

In examining the role of parents as a frontline safeguard for online safety, consideration has also been given to the question of whether children should have access to digital devices at all. However, this perspective must be balanced with the recognition of children's rights to access information and participate in the digital world (see [earlier section](#)). A total ban of devices or social media would be a significant policy direction for Government to take and a more moderate focus of ensuring that children can safely exercise digital rights, and equipping parents with the necessary knowledge and support to guide them responsibly is probably more practical. Although Ministers have acknowledged this in their responses, there remains a gap in concrete examples of how these principles will be translated into effective practice.

This section has largely covered parents and caregivers in a home environment, but it is important to acknowledge that for some children who are in the care of the Minister there will be a corporate parent involved in their care and therefore the responsibility for prevention and protection from online harms extends to the State and its appointed carers. Corporate parenting carries a duty to safeguard children's wellbeing across all domains, including their digital lives. This means that the Government needs to ensure that foster carers, residential care staff, and other professionals are equipped with the knowledge, tools, and support to monitor online activity, educate young people about digital risks, and intervene when necessary to ensure that young people in foster care are not disadvantaged.

---

<sup>295</sup> [Ibid](#), p. 1

<sup>296</sup> [Transcript – Online Harms Review Public Hearing - Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.16 and p. 19

<sup>297</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.14

## Safety-by-Design

During the course of this review, the Panel has explored the concept of safety-by-design, i.e. a proactive approach to online safety that prioritises the needs and rights of children from the outset of digital product development. Rather than placing the burden solely on families, schools, or individual users, safety-by-design shifts responsibility to technology developers, digital platforms, and regulatory frameworks to ensure that online environments are inherently safe and age-appropriate. An OECD report explains that:

*Digital safety by design for children is emerging as a concept that could point the way towards innovation that is both beneficial and responsible, placing children's safety and well-being at the forefront.*<sup>298</sup>

The Minister for Children and Families advised the Panel that integrating digital safety-by-design into government policymaking is essential to safeguarding children in today's digital landscape.<sup>299</sup> This approach involves embedding safety principles into the development, procurement, and regulation of technologies used by children. Platforms should be designed to default to safety, offering:

- Age-appropriate privacy settings;
- Clear and accessible reporting tools; and
- Content moderation systems that prioritise child protection.

Furthermore, in addition to safety, one aspect that has been indicated by research in relation to new technologies such as A.I is that they can contain biases which can impact a users' digital experience. Research has found that automated decision-making in online services often discriminates against characteristics such as gender, age, ability, language, ethnicity and socioeconomic status. This can create obstacles for the enjoyment of digital opportunities by all children.<sup>300</sup>

The Panel also examined the principle of age-appropriate design, a key component of safety-by-design. According to the UNCRC's General Comment No. 25, the risks and opportunities children face in digital environments vary significantly depending on their age and stage of development. Therefore, the design of digital services must be informed by research and tailored to children's evolving capacities.<sup>301</sup>

General Comment No. 25 further highlights the risks associated with leisure time spent online, noting that children may be exposed to harm through:

- Opaque or misleading advertising; and
- Highly persuasive or gambling-like design features.

---

<sup>298</sup> [‘Towards Digital Safety by Design for children’](#), OECD Digital Economy Papers, June 2024 (No.363), p.7

<sup>299</sup> [Letter – Minister for Children and Families to CEHA Panel following public hearing – 9<sup>th</sup> June 2025](#)

<sup>300</sup> [‘The children's rights-by-design standard for data use by tech companies’](#), P. Hartung, UNICEF, Good Governance of Children's Data project, November 2020, p. 4

<sup>301</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021

To mitigate these risks, the UNCRC calls on States Parties to adopt data protection, privacy-by-design, and safety-by-design measures, ensuring that commercial interests do not override the rights and wellbeing of children.<sup>302</sup>

*The Committee encourages States parties to introduce or update data protection regulation and design standards that identify, define and prohibit practices that manipulate or interfere with children's right to freedom of thought and belief in the digital environment, for example by emotional analytics or inference.*<sup>303</sup>

## Government led action

One of the distinct responsibilities for the Government in respect of the challenge posed by the digital environment is outlined in General Comment No. 25:

*The digital environment was not originally designed for children, yet it plays a significant role in children's lives. State parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration.*<sup>304</sup>

Therefore, per the obligations under the UNCRC, the Government of Jersey, as the relevant State party has responsibilities in this digital space to safeguard and prioritise children's wellbeing.

Jersey has also ratified the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography which requires states to ensure that they take measures to prevent online sexual abuse and exploitation of children.<sup>305</sup>

The Panel has already explored how existing policy in Jersey provides protection to children from various online harms and threats, for example, in educational settings and the Jersey's Children First practice framework in CYPES. We have also learned that there is a cross-Ministerial Group that has been established to coordinate the Government's work in relation to online safety.

In addition to the cross-Ministerial Group, there is a proposal for a cross-departmental officer group to support the Ministerial group. It is unclear how these new groups will work in partnership with other existing coordinating bodies and groups. In a letter to the Panel on 10<sup>th</sup> March 2025 the Minister for Children and Families advised that the bodies which had oversight of the key considerations that are relevant to policy and practice regarding online harms were:

- the Children's Outcome's Executive Committee;
- the Corporate Parenting Board; and
- the Safeguarding Ministerial Group

It was stated that these groups provided Ministers and senior officers opportunities to share and make connections between different ministerial policy agendas.<sup>306</sup> A short summary of these groups are shared below:

---

<sup>302</sup> [Ibid](#), p.18

<sup>303</sup> [Ibid](#), p.11

<sup>304</sup> [Ibid](#) p. 2-3

<sup>305</sup> [Written Submission – Children's Commissioner for Jersey](#)

<sup>306</sup> [Letter – Minister for Children and Families – 10<sup>th</sup> March 2025](#)



- The purpose of the [Children's Outcomes Executive Committee](#) is to oversee cross-Government policy development and monitor the CYPF Plan. This Committee meets twice a year, is chaired by the Minister for Children and Families, and its membership is made up of the Ministers named as 'responsible Ministers' in the [Children and Young People \(Jersey\) Law 2022](#). The [Terms of Reference](#) is available on the government website.
- The Corporate Parenting Board, established as a statutory requirement of the [Children and Young People \(Jersey\) Law 2022](#) has responsibility for children in care and is also chaired by the Minister for Children and Families. The membership of the board includes various Ministers, a representative from the Comité de Connétables, senior Government officials, representatives of children in care and care leavers, and representatives from the voluntary sectors, and the Foster Carers Association. The [Terms of Reference](#) is available on the government website.
- The Minister also advised the Panel that there were two levels to the Safeguarding Partnership Board, namely the executive board (which is chaired by and independent off-Island Chair) and a Ministerial level board. The Panel was unable to find further information about this group.<sup>307</sup>

The Panel was interested to understand the Government's approach to their overall responsibility for leading the legislation and policy to provide protection for children from online harms. The Assistant Minister for Children and Families opined that "*I think it is about empowering citizens rather than doing things to people.*"<sup>308</sup>

In a public hearing, in response to queries about age-appropriateness of content, and links to Children's Rights, it was emphasised that the Government used a multidimensional approach:

**Assistant Director of Policy:**

*If I may, the approach is one of a multiplicity of different approaches and layers. We have talked about supporting parents to play their part and understanding what they can do to help with age appropriateness, and as a parent I know that is not easy sometimes. We have talked about technical fixes and solutions in order to keep young people safe, and we have also referenced changes in the legislation that are going on. Your question is about rights and what sits above all of that is Jersey is part of the U.K. party in terms of the signatory to the U.N.C.R.C. We take that very seriously and play our part in the rolling 7-year review of our commitment to the U.N.C.R.C. and we continue to do that. We are doing more than one thing. I think it is also tied into the conversations and discussions with young people is a constant ear for should we be doing more, and the nature and the extent of that risk, balanced with the nature and extent of some of the opportunities offered by the online environment.*<sup>309</sup>

The Panel was also advised that data collected from surveys such as the Jersey Opinions and Lifestyles Survey and the Children and Young People's Survey is used to influence development of policies and procedures.<sup>310</sup> The Minister for Children and Families highlighted

---

<sup>307</sup> **Note:** During factual accuracy checking it was clarified that Ministerial oversight is provided by Safeguarding Responsible Ministers whilst Safeguarding Partners are government chief officers named in law with responsibility for delivering safeguarding strategy, improvement and practice.

<sup>308</sup> [Transcript – Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.5

<sup>309</sup> [Ibid](#), p.30-31

<sup>310</sup> [Ibid](#), p.18



the importance of engaging with children and young people on this topic and said that “e-safety” would be discussed at the School Council Network and output would be fed back to Ministers at the next meeting of the Children’s Outcomes Executive Committee for further action.<sup>311</sup>

The Panel previously noted in its ‘[Policy](#)’ section that while online safety is addressed across a range of Government policies, these efforts lack a cohesive, interconnected framework. It has been proposed that the BASC (Building a Safer Community) strategy could serve as an overarching approach to unify these initiatives. The Panel recognises that well-designed policy is a powerful mechanism for protecting children from online harms. When thoughtfully developed, policy can support safer digital environments while maintaining access to the positive aspects of technology. However, despite the presence of numerous structures and channels, a more integrated strategy is needed to effectively capture and coordinate these efforts.

Furthermore, as part of a broader strategy to promote wellbeing and resilience among children and young people, the Government has advised that it will also address online safety within the wider context of healthy development and through the work that schools and youth clubs already undertake. This includes supporting enticing alternatives to screen time through the forthcoming Play Strategy and other initiatives that encourage physical activity, creativity, and social engagement.<sup>312</sup> Public Health Jersey has recommended improving access to free, inclusive activities, such as sport, arts, and community programmes, as a means to offering positive substitutes for screen-based leisure and strengthening protective factors.<sup>313</sup>

## Role of Digital Platforms

The Minister for Children and Families advised the Panel that there should be greater onus on digital platforms to flag up inappropriate online behaviour, however, he was unclear about the legal mechanisms through which this could operate in Jersey. We copy below an exchange between the Minister and the Chair of the Panel from the public hearing on 23<sup>rd</sup> May 2025:

***The Minister for Children and Families:***

*I think that part of that is the ... there is the platform. You have got the platform owners, who to some extent should be looking for trends in things like that. If somebody has suddenly contacted 380 children in a week, you would have thought that that is abnormal. I know that people use the internet a lot, but you would have thought that they can use ... just as they use algorithms to select our Netflix or whatever, they should be able to use algorithms to spot potential predators.*

***Deputy C.D. Curtis:***

*Is this not where legislation comes in, to define ...*

***The Minister for Children and Families:***

*Yes, that is where the legislation comes in, to force them to do that.*

***Deputy C.D. Curtis:***

*But you do not think that is necessary?*

---

<sup>311</sup> [Letter – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

<sup>312</sup> [Letter – Minister for Children and Families – 10<sup>th</sup> June 2025](#)

<sup>313</sup> [Written Submission – Online Harms Review – Public Health Jersey](#)

***The Minister for Children and Families:***

*I do think that is necessary.*

***Deputy C.D. Curtis:***

*You do, for the ...*

***The Minister for Children and Families:***

*Yes. That is what I am explaining, so we should be able to force the owners of these platforms to do these things.*

***Deputy C.D. Curtis:***

*But that was the attempt of the Online Safety Act in the U.K.*

***The Minister for Children and Families:***

*But I would have thought our own legislation would be able to do that.*

***Deputy C.D. Curtis:***

*We do not have any legislation to ...*

***The Minister for Children and Families:***

*We have the computer misuse legislation already.*

***Deputy C.D. Curtis:***

*So you think that that would be sufficient?*

***The Minister for Children and Families:***

*It may or may not. I am not a lawyer, but it is certainly something that needs to be looked at.<sup>314</sup>*

The Panel does not believe that the Computer Misuse (Jersey) Law 1995 could be used to put obligations on the owners of social media platforms, for example, to ensure that they put in place measures to spot potential predators. However, suggest that the Government consider formally assessing this position to determine potential options.

During questions about age verification the Minister for Justice and Home Affairs highlighted that liaising with digital platforms would come under the jurisdiction of the Department for the Economy. The Panel was advised that:

*[...] the justice system, as it operates in Jersey, is sort of geographically linked to the Island and it operates at the speed of the justice system, which is not immediate. So the question of how you manage global providers, and their relationship with content, is not something really that you can do with the criminal justice system in a small jurisdiction. It is something that requires the negotiation and engagement that I think the Economy Department has been working on.<sup>315</sup>*

---

<sup>314</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.10

<sup>315</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.4

This reflects the broader challenge of regulating multinational tech companies from a small jurisdiction like Jersey. The Minister for Sustainable Economic Development echoed this, noting that take down requests often rely on informal networks and cooperation:

*It is really important from a small jurisdiction's perspective that these very large companies do listen to us and do act on our wishes... we have generally been able to work with those large platforms where takedown requests have been needed.*<sup>316</sup>

The Minister for Sustainable Economic Development had pointed to this being the responsibility of the Information Commissioner:

***The Connétable of Grouville:***

*We have already discussed the fact that the internet is global and crosses many borders. How do we ensure Jersey's rules of takedown requests are effective when content is hosted overseas?*

***The Minister for Sustainable Economic Development:***

*That goes back to my previous answer about that is the work of the Office of the Information Commissioner to develop their own networks, both formal and informal to do that. I myself spoke with an executive of Facebook during the Global Privacy Forum to say that it is really important from a small jurisdiction's perspective that these very large companies do listen to us and do act on our wishes in terms of takedown requests, et cetera. My understanding to date is that we have generally been able to work with those large platforms where takedown requests have been needed.*

***Assistant Minister for Sustainable Economic Development:***

*We are not aware that they are not honouring their own terms of use, so you may be aware Facebook, for example, has community standards. We are not generally aware that they are not honouring their own rules as such. That, I think, is the first recourse.*<sup>317</sup>

As per the Panel's previously noted finding, this response points to the responsibility of platforms as the guardians of content, and the Panel has recommended that the Government should clarify its position on legislating for online content governance.

In a report by the Digital Futures for Children Centre, they reference that the UNCRC's General Comment No. 25 makes it clear that national administrative authorities, legislative bodies and courts of law have the fundamental responsibility for setting and enforcing the standards to which all, including the private sector, are to be held. The report states that:

*This means that it is not the role of private enterprises to establish their own criteria and processes for determining what might or might not be in the best interests of the children who may be impacted by their activities; rather, they are obliged to ensure that their services meet the guidance or standards set by the state and / or by the Committee [on the Rights of the Child].*<sup>318</sup>

The report goes on to say that:

---

<sup>316</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.8

<sup>317</sup> [Ibid](#), p.8

<sup>318</sup> Sonia Livingstone et al., [The Best Interests of the Child in the Digital Environment](#), Digital Futures for Children Centre, March 2024, p.16

*...in the same way that manufacturers of products not designed for consumption by children are obliged to take effective measures to prevent children coming to harm from contact with them, it remains the full responsibility of digital service providers to take needed measures for the digital environment.*<sup>319</sup>

The OECD also recognises digital service providers as having an essential role in providing a safe and beneficial digital environment for children. One OECD report stated that:

*Ideally, when designing digital spaces, digital service providers would find and implement effective ways to protect children from harm whilst providing them with opportunities to enjoy the benefits of the digital environment.*<sup>320</sup>

It was also highlighted by the Digital Futures for Children Centre that:

*Many companies 'anticipate' regulatory demands by making changes during the progression or transition of new legislation, either to make the case that they do self-regulate, or sometimes to set the regulatory norms early.*<sup>321</sup>

Public sentiment collected in submissions to the Panel were fairly scathing of digital platforms, often citing corporate motives were prioritised at the expense of user health and wellbeing:

*How have we allowed society to be ruled by giant tech companies who make endless profits from allowing children to be exploited in this way? It is clearly wrong.*<sup>322</sup>

A number of written submissions referenced that social media operates in a distinct way in comparison to other digital platforms, often describing its influence using terminology associated with addiction:

*Online safety has now gone beyond 'digital wellness' or 'teaching your child to use social media safely'. Social media is not a simple tool. It is a powerful addiction-driving giant that is quite bluntly stealing our children's childhoods and has created a cataclysmic boom of late teens and young adults who are anxious and depressed (I refer to the release of research in October 2024 from Oxford University entitled "Brain Waves").*<sup>323</sup>

One submission from a 16-year-old said:

*Online safety training, and handing out pamphlets, is a joke. We know the rules but that doesn't stop anything. We know phones are designed by silicon valley millionaires who know how to mess with our brains - and even though we know this, we still don't really put them down, but isn't this the point?*<sup>324</sup>

Former Information Commissioner for Jersey and Guernsey, Emma Martins, said that:

*There is increasing and particular concern about children and young people using social media platforms. Our children and young people are becoming addicted and are being manipulated by design. Their attention is being treated as a resource to be*

---

<sup>319</sup> [Ibid](#), p.16

<sup>320</sup> ['Towards Digital Safety by Design for children'](#), OECD Digital Economy Papers, June 2024 (No.363), p.7

<sup>321</sup> S. Wood, ['Impact of regulation on children's digital lives'](#), Digital Futures for Children Centre, May 2024, p.11

<sup>322</sup> [Written Submission – Anonymous 16](#)

<sup>323</sup> [Written Submission – Online Harms Review – Victoria O'Neil](#)

<sup>324</sup> [Written Submission – Online Harms Review - Anonymous 13](#)

*profited from. Can any of us think of another area of young people's lives where such risk, exploitation and harms are accepted? It is both morally and legally unacceptable for any of us, particularly the young, to be commodified, yet that is the business model we have allowed to dominate our lives.*<sup>325</sup>

This submission also suggested that *"The burden of proof should not lie with those of us who seek to protect children from harm, it should lie with those who are building products which are being targeted at, and consumed by children to demonstrate and evidence that their products are safe."*<sup>326</sup>

There is a debate as to whether social media platforms are 'curators' or 'conduits' of digital content, as platforms often use algorithms to recommend content posted by users to others. In the written submission to the Panel from JOIC, they highlight that social media platforms usually expressly state that they are not responsible for content uploaded by users, albeit it may contravene the terms of use of the platform as set by the provider.<sup>327</sup>

The U.K.'s Select Committee [i.e. the House of Commons' Science, Innovation and Technology Committee] report of '[Social media, misinformation and harmful algorithms](#)' found that the advertising-driven business models of social media companies incentivised the creation and promotion of content that performs well, regardless of its truthfulness or harm potential. Amongst the report's conclusions, they said that it is vital that platforms are held responsible for the algorithmic spread of misleading or deceptive content that can radicalise and harm users. The UK's HoC SIT was critical of the UK's OSA and called for a more robust and principle-based approach to regulation which acknowledged the curatorial power of digital platforms and holds them accountable for the content they promote.<sup>328</sup>

#### FINDING 52



There is a consensus that protecting children from online harm requires a societal approach, involving collaboration across multiple sectors. However, a key challenge includes defining the scope of the response, particularly whether it should be locally tailored to Jersey or aligned with international regulatory frameworks.

#### FINDING 53



Enticing alternatives to screen time are important to encourage physical activity, creativity, and social engagement. Public Health Jersey has recommended improving access to free, inclusive activities, such as sport, arts, and community programmes, as a means to offer positive substitutes to screen time.

#### FINDING 54: Key Finding



A key challenge is the lag between technological innovation and the implementation of effective safeguards for online safety. The Panel's review has gathered evidence indicating that digital platforms should bear greater responsibility for designing their services to be suitable and safe for children, including addressing addictive behaviours and identifying and flagging inappropriate online behaviour. Whilst some platforms may anticipate regulatory demands and "self-regulate" the UNCRC has made it clear that it is the role of

<sup>325</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>326</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>327</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>328</sup> '[Social media, misinformation and harmful algorithms](#)', Science, Innovation and Technology Committee, House of Commons, 11<sup>th</sup> July 2025

governments to set the standards for a safe digital environment that is in the best interests of children.



**RECOMMENDATION 27**

The Minister for Children and Families should ensure that the draft Play Strategy includes consideration of how the Government of Jersey could support initiatives that provide young people with a variety of free and inclusive alternatives to screen time.



**RECOMMENDATION 28**

The Government of Jersey should initiate policy development to explore effective legislative approaches that place greater accountability on digital platforms, ensuring their operations are guided by principles of safety and rights by design.



## **What action can Jersey take to provide children with a safer digital future?**

To provide children with a safer digital future, the Government of Jersey should take a proactive approach to online safety that reflects both global best practice and local context. This section will explore recommendations that include ways to create a strong foundation for Islanders' digital lives and develop an internet safety, or online safety, strategy that will coordinate policy and governance on this matter.

### **Creation of an online safety strategy for Jersey**

As referenced in earlier sections of this report, with increasing screen time and digital engagement, children may face risks like cyberbullying, online grooming, exposure to harmful content, and privacy breaches. An internet or online safety strategy would help identify and mitigate these risks, especially for vulnerable groups.

When the Panel questioned Ministers in October 2024, the Minister for Sustainable Economic Development confirmed that the Government was in the early stages of thinking about an internet safety strategy, and it was emphasised that this would be a cross-Ministerial piece of work but that it was not in their current workstream. At the time the Minister also said:

*I think the issue is there is work going on out there at the moment and whether it is happening in schools, directly through the Education Department or whether it is happening through the Data Protection Authority and other such as Cyber Security Centre, there is a lot of work around internet safety going on but what we do not have is that single documented strategy for putting it all together, and I think it is a really good idea for us to look at that.*<sup>329</sup>

In public hearings and written correspondence in May – June 2025, Ministers were each asked whether there should be an Island wide strategy for protecting children from various forms of online harm. The responses are summarised below:

- **Minister for Education and Lifelong Learning:** supported the idea of an Island-wide strategy that involves all sectors of the community. However, cautioned against strategies becoming unused documents and advocated for a community-wide conversation that encourages shared responsibility, suggesting that the central question should be: *What do we want for our young people?*<sup>330</sup>
- **Minister for Sustainable Economic Development:** provided a similar response to that of October 2024 (as quoted above), he supported the idea of a strategy, provided that it was cross-Ministerial and referenced that the existing work of the Data Protection Authority would form part of it, however, said it was too early to provide any detail and that it was not part of any current workstream.
- **The Minister for Justice and Home Affairs:** suggested that there already was an unofficial strategy, in part because of the existing work in areas like corporate parenting

---

<sup>329</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.38

<sup>330</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.48

and safeguarding but acknowledged that the work was fragmented and that it needed to be refocussed and coordinated.<sup>331</sup>

- **Minister for Children and Families:** wrote to outline what a future online safety strategy should do but said that, because there was only a year left in this current political term, his focus would be to ensure families are effectively supported to navigate challenges relating to online and digital safety, rather than working on strategy development.<sup>332</sup>

The Panel did not feel that the Minister for Children and Families had directly answered the question in his written response and therefore the Chair questioned the Minister further in the States Assembly on 24<sup>th</sup> June 2025. The Minister confirmed that a strategy was important and that he was 100 percent supportive of one. He explained that the newly formed cross-Ministerial group would coordinate the approach to developing a strategy, however, his response reiterated the theme of the written correspondence with the Panel: that a strategy for online safety was a good idea for the future but it would not form part of the work he was focused on in the short term. He said:

*A cross-Ministerial group has now been established to co-ordinate the approach and develop a strategy on this matter, including any considerations arising from the Scrutiny Panel's review. I believe that this group will focus on actions, offer a tiny and important focus point for Government and an evolving area of policy development. My focus in this is to ensure families are effectively supported to navigate those challenges in the short term, rather than working on any other strategy. I accept that in order to develop our medium and future-term approach to this policy issue we need a sustainable, strategic approach. Any future strategy must avoid duplication of existing work and be agile enough to keep pace with rapidly evolving technology. It must also balance child protection with young people's rights to freedom, expression and digital access. I recognise there are other challenges to overcome that coincide with this issue, for example, alternatives to screens and mobiles in the shape of play spaces and I hope the play strategy will help in this aspect.*<sup>333</sup>

During the question session on 24<sup>th</sup> June 2025, the Minister for Children and Families also said:

*I think that a strategy is extremely important. We must help families and the children themselves deal with these online issues. What is always at the front of my mind in these things is that once a child or young person has seen a disturbing image that can be never removed from their mind. I think that is particularly important when we start to consider whether there should be a block on social media, for instance. I have my own personal view on that. I need to speak to other Ministers but my personal view is that I think we will have to, through the owners of these platforms, certainly bring in some restrictions on social media.*<sup>334</sup>

---

<sup>331</sup> [Transcript – Online Harms Review Public Hearing – Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025](#), p.36

<sup>332</sup> [Letter – Online Harms Review – Minister for Children and Families – 10<sup>th</sup> June 2025](#)

<sup>333</sup> Hansard – States of Jersey – 24<sup>th</sup> June 2025, [oral question 147/2025](#)

<sup>334</sup> [Ibid](#)

The Panel notes the Minister for Children and Families' suggestion of potential restrictions or a block on social media, which may be considered a contentious policy direction. At the same time, the Minister has indicated that his current focus is on short-term support rather than long-term strategic development. The Panel queries how these two positions align and whether they reflect a coherent approach to addressing online harms.

Some submissions to the Panel's review have referenced the need for the Government to produce an online safety strategy. Emma Martins opined that this was a significant cultural issue and that the Government has a responsibility to take action:

*There is also an urgent need for a government-wide vision and strategy and for a consistent approach to resulting actions. All citizens enter into a social contract with their government and the protection of those most vulnerable is necessarily a key part of that contract. I am of the opinion that this is one of the most pressing social and cultural issues of our time and the actions we take, or neglect to take, will ripple forward for many years, and impact many people.*<sup>335</sup>

A formal strategy would align efforts across government departments, schools, law enforcement, and health services. It would promote a proactive approach and clarify roles, responsibilities, and decision-making processes, especially around content moderation, data protection, and platform accountability. The need for a coordinated approach was highlighted to the Panel by the Information Commissioner, who explained:

*We have seen the scattergun approach too many times in history to know that we cannot just legislate for whatever we perceive the harm to be, shouting loudest at the time might be. So we would recommend a long-term holistic view with a focus on future threats and future protections, with the ability to adapt as needed as the environment changes. I think it is also important to say that we must recognise that online harms is not just about social media platforms and mobile devices or algorithms. It goes much deeper than that. It is about a myriad of information, misinformation, disinformation that young people are exposed to and including, but not limited to, sexual content, radicalisation, gang cultures, self-harm, suicide. You have seen other people talk about this. I think we should try and avoid, wherever possible, a reactive proposal that does not address the underlying problem, or worse, fail to provide the appropriate protections for those that we are trying to protect.*<sup>336</sup>

In the previous written correspondence to the Panel the Information Commissioner had advocated for comprehensive research that would inform future work:

*...we advocate for fulsome comprehensive research to take place so that together we can ensure that we fully understand the risks we face as an island community and so we can work to put a cohesive, proportionate and effective policy and regulatory framework in place that is fit for the island, and our children and, importantly, with them included in those discussions.*<sup>337</sup>

---

<sup>335</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>336</sup> [Transcript –Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.4

<sup>337</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

As previously explored, Jersey's data protection law includes a domestic purposes exemption, meaning it does not apply to individuals processing data for personal use, such as sharing photos or comments on social media.<sup>338</sup> This legal gap leaves children and other users exposed to harmful online behaviour that falls outside regulatory oversight. An online safety strategy must therefore extend beyond data protection and address broader risks in the digital environment.

The Panel therefore makes the point that any strategy has to do more than tie together the existing work from the Data Protection Authority, the Cyber Security Centre and the Education department (as suggested by the Minister for Sustainable Economic Development in October 2024) and the Minister for Children and Families comments about the cross-Ministerial group offering a *"tiny and important focus point"* and that his area of focus would be solely supporting families to navigate short term challenges. This fragmented approach suggests the need for a coherent, long-term, and cross-government strategy that sets out a clear vision for online safety.

International obligations further reinforce this need. The UNCRC's General Comment No. 25 calls on states to allocate public resources to support children's rights in the digital world.<sup>339</sup> It highlights that children's rights are interdependent and indivisible, requiring comprehensive protection. Jersey must ensure its digital policies align with these international obligations and adopt a rights-based approach that respects, protects, and fulfils all aspects of children's rights online.

Stakeholder input also supports this direction. The NSPCC's submission to the Panel highlighted that whilst *"statutory regulation is a fundamental part of keeping children safe online, it is not the only lever available to Governments"*<sup>340</sup> and the need for a *"holistic framework"* was required. A strategy would enable Jersey to respond with evidence-based interventions and targeted public education to risk and areas of public concern.

As other jurisdictions implement robust online safety laws, Jersey risks falling behind without its own framework. A strategy would help ensure compatibility with international regulations and tech platforms, while also reinforcing Jersey's commitment to digital safety and wellbeing. As Emma Martins has noted, *"we only have balance when we have safety."*<sup>341</sup> Therefore, as suggested by the Children's Commissioner:

*the Government needs to set out what its approach is in terms of online safety. This needs to be a coherent and cross-government approach, focused on respecting, protecting and fulfilling children's rights in the digital world.*<sup>342</sup>

The strategy should include specific consideration of protections for vulnerable children and children with disabilities and, also, address the full scope of children's digital access, not just phone use in schools, but internet and social media access on any device, whether children are in a CYPES setting, at home, or elsewhere. Online safety is not a siloed issue, it is a public

---

<sup>338</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>339</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.5

<sup>340</sup> [Written Submission – Online Harms Review – NSPCC Jersey](#)

<sup>341</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>342</sup> [Written Submission – Children's Commissioner \(follow up\) – 30<sup>th</sup> July 2025](#)

health concern that demands a societal approach and shared responsibility across families, educators, policymakers, and technology providers.

The Panel suggests that any strategy must include the following elements, all of which are explored in the final sections of this report:

- Define expectations for digital skills;
- Include views of the public, particularly co-design with children and young people;
- Clarify the role of legislation;
- Clarify the role of data protection in relation to online harms;
- Improve enforcement and accountability;
- Cross-Government co-ordination;
- Consider the school curriculum and CYPES online safety policy;
- Ensure that there is support for children and young people impacted by online harm;
- Engage businesses and digital platforms; and
- Look to best practice in other jurisdictions.

#### **FINDING 55**



Ministers have expressed support for the development of an online safety strategy, and the Panel has been informed that the cross-Ministerial group intends to begin coordinating this work. However, based on current indications, the Panel understands that significant long-term action may not be initiated within the remainder of the current political term.



#### **RECOMMENDATION 29: Key Recommendation**

The Government of Jersey should prioritise the development of a comprehensive online safety strategy, with a particular emphasis on safeguarding children. Such a strategy should be grounded in a rights-based framework, incorporate cross-government collaboration, be forward-looking, and capable of addressing current challenges while remaining adaptable to the evolving digital environment.

## Define expectations for digital skills

As noted at the outset of this report, the Panel considers clear definitions and classifications of online harms essential to create a shared understanding across different stakeholder groups. We suggest that a similar principle applies to the expectations for digital skills.

The consultation undertaken by the Government of Jersey in 2022 which informed the [Children and the Digital World report](#), identified that there were opportunities to raise skill levels in the following areas:

- Digital literacy (skills to make good choices such as awareness and digital thinking);
- Digital etiquette (screen time and how we treat others);
- Digital wellness (digital downtime and support networks); and
- Digital security (use of personal information).<sup>343</sup>

As a follow up to the Children and the Digital World report, the Government published a new [Digital Education Strategy](#) (hereafter the 'DE Strategy') in 2022, however, references to these four points in the DE Strategy are limited. The DE Strategy has a strong focus on linking digital skills with industry, however, in respect of specific references to digital literacy it states that there should be a "baseline"<sup>344</sup> for this and that, also, that "Pragmatic digital literacy was felt lacking in schools – "kids can code but can't do the fundamentals"<sup>345</sup>.

In a letter to the Panel, the Minister for Children and Families stated that the DE Strategy:

*[...] not only supports the development of digital skills for young people and educators, but places wellbeing and responsible digital citizenship at its heart. This includes building a common framework of age-appropriate digital and non-digital life skills, from early years to post-16 education.*<sup>346</sup>

Consideration of whether children and young people had necessary digital tools and skills was highlighted to the Panel by the Children's Commissioner:

*Even though children are seemingly skilled at using digital tools, this does not mean that they are digitally literate. It is important to recognise that they still need support and guidance for developing their critical evaluation skills.*<sup>347</sup>

The Panel has understood the concept of "digital literacy" to be about the technical skills needed to use digital tools. It differs from "digital citizenship" in that it emphasises functional proficiency and understanding of digital content rather than about using technology ethically and responsibly. Because both concepts involve navigating digital environments and making informed choices online, there is a risk they may be conflated, especially when discussions focus broadly on "digital skills" without distinguishing between technical proficiency and ethical engagement.

As referenced in the section discussing definition for online harms, the same principle applies relating to the requirement for a common foundational language to facilitate a shared

---

<sup>343</sup> [Children and the Digital World](#), Government of Jersey, May 2022, p.29

<sup>344</sup> [Digital Education Strategy, Government of Jersey, November 2022](#), p.12

<sup>345</sup> [Ibid](#), p.16

<sup>346</sup> [Letter – Online Harms Review – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

<sup>347</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.3



understanding as there could be subjective interpretations of what digital skills and digital literacy mean to different people, particularly between children and adults.

The Children and the Digital World report had referenced that the feeling of “too much” screen time increased with children’s age and suggested that:

*This self-awareness reflects a strong level of the digital citizenship elements of digital literacy and digital etiquette, which include core skills such as awareness, critical thinking and decision making to support good decision making and positive online behaviour.*<sup>348</sup>

However, it also detailed that “while adults may be able to separate their online and offline worlds, these are fully integrated for children and young people and digital engagement has been accelerated due to COVID-19”.<sup>349</sup> This suggests that adults were able to put a degree of separation between their online world and their offline world, and that this was a good thing for their health and wellbeing. However, children’s offline and online lives were more interconnected with each other. The report shared the importance of investing in educating adults in order to support children with online safety and digital skills:

*Alongside this, is the investment in ongoing support and engagement across the community, primarily focused on parents, carers and family members that have childcare responsibilities. These individuals influence children’s online engagement and there is an opportunity to equip them at an early stage to help prevent the potential harms of the digital world.*<sup>350</sup>

In relation to education delivery the Children and the Digital World report detailed the need for investment in IT equipment and in maintaining education practitioners’ levels of digital literacy. The report states that it is essential that educators are proficient in the safe delivery of digital education.<sup>351</sup> However, as part of the Panel’s review of Secondary Education Funding (published as [S.R.10/2024](#)) the Panel referenced digital literacy as part of curriculum discussions and highlighted that whilst technology impacts all aspects of learning and development, school budgets for Information and Communication Technology had not changed in ten years.

During the Panel’s review of Secondary Education Funding the Minister for Education and Lifelong Learning also acknowledged the importance of technology for students to become digital citizens and indicated that “significant investment”<sup>352</sup> was needed in order for teachers and students to be able to effectively use technology for education in the immediate and long term.

In the evidence collected from the JOIC, the Panel was informed about the outreach programmes they provided, which included working with the Education Department in CYPES. It was emphasised that digital education should include information about consequences of online behaviour, for example, protecting privacy and future opportunities. The Information Commissioner advised the Panel that:

---

<sup>348</sup> [Children and the Digital World](#), Government of Jersey, May 2022, p.19

<sup>349</sup> [Ibid](#), p.19

<sup>350</sup> [Ibid](#), p.6

<sup>351</sup> [Ibid](#), p.14

<sup>352</sup> ‘[Secondary Education Funding](#)’ (S.R.10/2024), Children, Education and Home Affairs Scrutiny Panel, 9<sup>th</sup> December 2024, p.51-52

*Given the exponential advances and uses of technology, it is critical, now more than ever, that we take steps to educate young people on how online behaviours can affect their opportunities in later life and provide them with the tools to protect themselves against the many harms associated with a digital environment and ensure they are empowered and equipped with the tools to protect their own personal information and that of others as they enter employment.*<sup>353</sup>

For children, achieving digital literacy, could be supported through the school curriculum or their contact with other services or organisations. However, as referenced in the earlier section about '[Parents, caregivers and family members](#)' it has been highlighted to the Panel that supporting parents, carers, educators, and other adults in developing digital literacy is also essential in order to create an informed and responsible digital culture that helps to protect children online, but they need to be given the tools and support to do this.

In the [written submission](#) to the Panel from the Safeguarding Partnership, they noted that following the joint conference (with the NSPCC in November 2024) attendees had provided ideas about priority areas to be progressed in Jersey. One of the main areas was around Education and Awareness, and the following points were noted:

- **In Schools:** Establishing a standardised online safety curriculum, integrating Personal Social Health Economic education (PSHE), and introducing early intervention strategies.
- **For Parents & Carers:** Providing accessible workshops and resources to help families understand and mitigate online dangers.
- **For the Community:** Launching public awareness campaigns to encourage open conversations and collective action against online harm.<sup>354</sup>

The UNCRC's General Comment No. 25 on children's rights in relation to the digital environment is in alignment with these ideas and advocates for targeted training for parents, educators, and caregivers, which is grounded in research on child development:

*Training and advice on the appropriate use of digital devices should be given to parents, caregivers, educators and other relevant actors, taking into account the research on the effects of digital technologies on children's development especially during the critical neurological growth spurts of early childhood and adolescence.*<sup>355</sup>

Therefore, the Panel has found that a variety of digital skills are recognised as an important aspect in the ability to use technology to find, create and communicate information safely and responsibly, however, it needs to be considered within a cultural context, not just focussing on children and young people but also the adults that support them.



#### FINDING 56

The Government of Jersey has acknowledged the significance of digital education, yet there remains a lack of clear guidance around defining digital literacy expectations. While many children are proficient in using digital devices

<sup>353</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>354</sup> [Written Submission – Online Harms Review – The Safeguarding Partnership Board](#)

<sup>355</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#),

Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.3

and platforms, this competence does not automatically translate into true digital literacy.



**RECOMMENDATION 30**

As part of any future strategy development, the Government of Jersey should take steps to define 'digital literacy' and 'digital citizenship' and what these mean for all Islanders, in order to improve online safety and Jersey's digital culture.



**RECOMMENDATION 31**

The Minister for Education and Lifelong Learning should support digital literacy for all and make efforts to embed digital literacy into any lifelong learning ambitions for the Island. This includes targeted support for adults, in order to allow them to support children's digital development.

## Include views of the public, particularly co-design with children and young people

In an earlier [section](#) the Panel noted the consideration of whether there is a disconnect between adult assumptions about online risks and children's own perceptions of danger and highlighted the importance of grounding policy and educational initiatives in children's lived experiences and perspectives. An effective online safety strategy must be shaped not only by policymakers and regulators, but by the lived experiences of children, young people, and the wider public. Their voices offer critical insight into the realities of digital life and the risks that policy must address.

### Children's Right to Be Heard

Article 12 of the UNCRC states that children have the right to participate in decisions that affect them. The Children's Commissioner for Jersey has emphasised that it is "*absolutely critical that children are involved*"<sup>356</sup> in shaping digital policy. This includes ensuring children have opportunities to express their views on matters related to their use of digital technologies, including how digital platforms affect their lives, education, and well-being.<sup>357</sup>

The UNCRC's General Comment No. 25 further reinforces that children's participation in digital spaces must be recognised and supported, including their views on how platforms impact their education, wellbeing, and safety. This was acknowledged by the Minister for Education and Lifelong Learning who emphasised that young people had to be given some ownership of their own safety.<sup>358</sup>

A key point raised by the Children's Commissioner was that understanding children's views of online harm is an important place to start:

*...simply asking children, have you seen inappropriate sexual content without an understanding of what children determine to be inappropriate sexual content, the answers to those questions do not make a lot of sense. I think anything that we ask children, how we collect their views, needs to understand their understanding of online harm. I think that is potentially the place where we need to start.*<sup>359</sup>

### Insights from Local Data

The JCYPS has tracked screen use and digital engagement over time, with findings from 2019, 2021, and 2024 revealing significant shifts in how children interact with technology. Any trends help inform local policy, but numbers alone are not enough, and the Panel was advised that talking to young people is essential to interpreting the data meaningfully. Furthermore, initiatives like the school council network and YES (Youth Enquiry Service) have provided valuable platforms for young people to shape digital policies. The Panel was also advised that

---

<sup>356</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.6

<sup>357</sup> [Written Submission – Children's Commissioner for Jersey](#)

<sup>358</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.13

<sup>359</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.6

engagement around e-safety in schools, and joint working with the Information Commissioner was planned.<sup>360</sup>

### Public Concerns and Parental Voices

In submissions received by the Panel, parents and caregivers have called for clearer guidance and support in navigating online risks. Their concerns reflect a broader public demand for transparency, accountability, and effective safeguards. However, it has been suggested to the Panel that overly restrictive measures may backfire. The Information Commissioner warned that stringent controls could drive children toward unsupervised or secretive online behaviour:

*We are also concerned that imposing stringent restrictions could lead to children seeking unsupervised or secretive ways to access online platforms which, in turn, may actually increase the risk of exposure to harmful content. It may also make it less likely for children to seek out help or guidance when they do encounter harmful content.*<sup>361</sup>

Co-designing an online safety strategy that actively includes public input, especially from children and young people, is essential to ensure the strategy is relevant, practical, and responsive to real-world harms. As referenced earlier, children's experiences and patterns of internet use are different from adults, therefore relying solely on adult perspectives risks could overlook the unique vulnerabilities and concerns of younger users. Research into how children and young people use the internet, and what they consider to be harmful within those spaces would be helpful to capture the nature and impact of online harms. Furthermore, meaningful participation in strategy development strengthens its effectiveness and increases the likelihood of public support, trust, and long-term engagement.



#### **RECOMMENDATION 32**

To shape an effective online safety strategy and understand the nature and impact of digital harms affecting children and young people, the Government of Jersey should research how children and young people engage with the internet and what they perceive as harmful within online environments.

<sup>360</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.20

<sup>361</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

## Clarify the role of Legislation

A comprehensive online safety strategy must clearly define the role of legislation in safeguarding users, particularly children, from digital harms. Legislation provides the structural framework for enforcement, accountability, and rights protection in the online environment. Without a clear legislative framework, efforts to regulate harmful content, protect vulnerable users, and ensure platform compliance risk being fragmented, inconsistent, or unenforceable.

In October 2024 the Panel questioned Ministers about their position on the policy of online safety. The Minister for Sustainable Economic Development explained that:

*As a matter of policy, effectively we want to see a free internet, free for expression, but we also want to see a safe internet, and that is where I try to strike that balance through particularly those 2 laws at the moment, the Telecommunications Law and the Data Protection Authority Law.*<sup>362</sup>

During the hearing in October 2024 the Minister for Justice and Home Affairs explained the ongoing work that the Government was doing to respond to the VAWG report recommendations which impacted online safety. This included amendments to the Sexual Offences Law, which will address intimate image abuse and cyberstalking. The Panel was advised that two parallel workstreams are underway: Justice and Home Affairs are developing criminal offences for digital harms, while the Department for the Economy is focusing on enforcement.<sup>363</sup>

During the public hearing with the Minister for Sustainable Economic Development in May 2025, it was acknowledged that while there was initial consideration of amending the Data Protection Law to enhance protections, legal advice led to the conclusion that a separate, more tailored piece of legislation would be more effective. It was explained that the new law would be lighter in scope than the U.K.'s OSA and would be designed to suit Jersey's specific needs. It would grant Islanders a legal right under Jersey law to request the removal of harmful online content, independent of existing platform terms of use. However, the timing for its introduction remains uncertain. It was stated that:

*It is really there to give Islanders the legal right under Jersey law to approach online providers, separate to the terms of use which already apply to them, to request that posts be taken down.*<sup>364</sup>

The Panel sought clarity on whether any legislative changes referenced by Ministers in relation to online safety would solely involve amendments to existing laws or would also include new standalone legislation. The Minister for Children and Families said:

*It is a mixture of both that they are intending, that they will have a law which enhances people's ability to have information taken down, but we will also enhance existing legislation. I mean, existing legislation is quite good. We have already had a prosecution, as you probably know, for A.I. (artificial intelligence) created images, and*

---

<sup>362</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.6

<sup>363</sup> [Ibid4](#), p.14

<sup>364</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.3



*the fact that that law was created some years ago, before A.I. generated images, I think just shows how well drafted those laws were in the first place.*<sup>365</sup>

The Minister for Children and Families also expressed the view that adding another layer of legislation is not necessarily the solution to addressing online harms. Instead, the Minister emphasised the importance of continuously reviewing and updating existing legislation to keep pace with emerging risks, in a public hearing he likened it to vaccines, which are only effective against known threats.<sup>366</sup>

In the public hearing in May 2025 the Assistant Minister for Children and Families indicated that public awareness was as important as legislation:

**Deputy C.D. Curtis:**

*Do you think with these devious people on the internet targeting children that there should be more legislation to protect children?*

**Assistant Minister for Children and Families:**

*I think we need to raise awareness of what the issues are and how people can be controlled and coerced over the internet. That is as much as important as creating new legislation, but certainly if we look at the suite of legislation which is available through data protection, we can create and empower people to be able to at least take images off the internet in a short space of time.*<sup>367</sup>

The Minister for Education and Lifelong Learning, was also cautious and emphasised that it was important to have clarity about what the legislation would address:

**The Minister for Education and Lifelong Learning:**

*... I am going to say it depends on what that legislation is. The legislation has to be clear as to what it will address. If it is clear as to what it addresses and works, then, yes, I would be very supportive of it. I think we have things that are already there that we need to emphasise more. There are lots of laws around online behaviour, around data protection, around what data is and how we use it. This is not a cop out in any way because this is what I mean, I would support any legislation that is effective and the right thing to do. I do not think we can just impose legislation from somewhere else for Jersey. I think we have an opportunity to do the right things that we want to do in a simple way if we had to take that on board. If it is the right thing to do, yes, I would support it.*<sup>368</sup>

The Minister for Sustainable Economic Development emphasised that the strengths of Jersey-led legislation:

*The laws that we have at the moment, both the Data Protection Law and the Telecommunications Law, where they have been really helpful, is that they have been designed, and certainly the Telecommunications Law and its more recent*

---

<sup>365</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.10-11

<sup>366</sup> [Ibid](#), p.41

<sup>367</sup> [Ibid](#), p.6

<sup>368</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.47

*amendments, to cope with the ongoing technological revolution, for want of a better word. Technology is constantly changing and particularly I think it is Article 51 where it has been designed specifically to cope with future technological changes as best it can without having to go back and always change a lot. That is a potential strength there. That is also one of the things that I think is a strength about us designing our own legislation is that we can make sure that it is fit for the future.*<sup>369</sup>

In summary, whilst the Government has commenced some work to develop new legislation relating to intimate image abuse, harassment and stalking, the Panel suggests that Ministers have indicated caution around wider legislation to address the sources of online harms. As we have found, Jersey's data protection legislation will not adequately address the full spectrum of online harms, particularly those arising from personal content sharing or harmful behaviour between individuals online (this is explored further in the [next section](#) of this report) and there is a risk that it could be considered more reactive, rather than proactive, in preventing harms from occurring in the first place.

### Challenges

In addition, the Panel has heard that legislation must be future-facing and be able to work with global frameworks to enable cross-border enforcement and cooperation. This is especially important for small jurisdictions like Jersey, where harmful content often originates from outside the Island's legal reach (see section on [Enforcement](#) below). By aligning with international standards and embedding child-specific protections, Jersey can strengthen its legislative foundation and ensure that its online safety strategy is both effective and equitable.

The UNCRC's General Comment No. 25 references that States parties should address the challenge of using legislation to regulate against technology and outlined that: "*Legislation needs to remain relevant in the context of technology advances and emerging practices.*"<sup>370</sup> Furthermore, the General Comment details the importance of international cooperation:

*The cross-border and transnational nature of the digital environment necessitates strong international and regional cooperation, to ensure that all stakeholders, including States, businesses and other actors, effectively respect, protect and fulfil children's rights in relation to the digital environment. It is therefore vital that States parties cooperate bilaterally and multilaterally with national and international non-governmental organizations, United Nations agencies, businesses and organizations specialized in child protection and human rights in relation to the digital environment.*<sup>371</sup>

The importance of international alignment was also highlighted to the Panel in the submission from the NSPCC:

*The best way to protect children is through globally aligned regulation which puts the responsibility upon tech companies to make children's online safety a priority.*

---

<sup>369</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.24

<sup>370</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.4

<sup>371</sup> [Ibid](#), p.20

*International harmony in regulation will help keep all children safer, raise standards globally, and show that we can be ambitious when talking about child safety online.*

*With the Online Safety Act now in force in the UK, alignment of regulatory requirements, whether via Jersey-specific legislation or other means, would likely offer the best form of online safety protection for children in Jersey.<sup>372</sup>*

While the NSPCC emphasised the value of international regulatory alignment to enhance child safety online, the Panel also recognised the broader implications of such alignment for Jersey's digital economy. This led to a discussion with the Minister for Sustainable Economic Development on whether diverging from international norms, by introducing Jersey-specific legislation, might pose challenges or opportunities for digital service providers operating across jurisdictions. The Panel asked the Minister for Sustainable Economic Development about the risk of regulatory fragmentation:

**Deputy H.M. Miles:**

*[...] One of the cited benefits of the E.U. (European Union) Digital Services Act is that it makes it easier for providers of digital services to set up in Europe and adhere to one set of rules across Europe. Do you think that Jersey having its own suite of legislation could potentially act as a disincentive to companies setting up here?*

**The Minister for Sustainable Economic Development:**

*I genuinely do not think so. Often, having a point of difference from the big norm, works the opposite way and gives you a competitive advantage. If our legislation was onerous in some way, the implementation for the digital business if we were making it difficult for them to work with Jersey, that would have an impact, but as long as our legislation is workable, then I do not see it like you tell it.<sup>373</sup>*

The Government of Jersey should ensure that it has considered its approach to legislating in order to protect children from online harms, ensuring that there is a balance between the legislative autonomy and flexibility that has been referenced by Ministers and ensuring that any legislation works together with legislation being developed elsewhere.

Should there be further legislation to address online harms?

In the [written submission](#) to the Panel from the Safeguarding Partnership, they said that following their conference focussing on Online Harms (in November 2024, jointly with the NSPCC) attendees had provided ideas about priority areas to be progressed in Jersey. One area was 'Legislation and Governance' and under that heading they shared the following:

- **Policy Alignment:** Strengthening Jersey's legal framework in line with the U.K. Online Safety Bill.
- **Tech Accountability:** Introducing stricter regulations for tech companies, including penalties for non-compliance.

---

<sup>372</sup> [Written submission – Online Harms Review - NSPCC Jersey – 21<sup>st</sup> March 2025](#)

<sup>373</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.33

- **Consistent Training:** Ensuring all organisations, schools, and agencies follow agreed safeguarding procedures.<sup>374</sup>

In public submissions to the Panel, there were calls for legislation to address online safety. One submission detailed:

*I am also extremely concerned about the lack of legislation around social media and smartphone use for children. There is an urgent need for stricter policies, including potentially limiting or banning social media for under-16s and ensuring that families in Jersey have access to simple, 'brick' phones that prioritize safety over social media and gaming distractions. Our children deserve to experience childhood without the constant pressures and risks posed by unrestricted digital access.*<sup>375</sup>

The Children's Commissioner advised the Panel that legislation should be a part of any framework or strategy aimed at tackling online harms:

*In my opinion, legislation is and has a critical role to play in any framework, or somebody mentioned the word "strategy" earlier on to address online harms. I think it needs to set out the standards of behaviour, activities and practices that, as a society, we believe are acceptable, as well as providing a very clear means for holding those who do not adhere to them to account and hold them robustly to account. But I think legislation is only one part of any framework or strategy and can only be one part.*<sup>376</sup>

In a public hearing the Information Commissioner advised that Panel that a decision was required regarding the approach to legislation:

*...there is a decision to be made between legislation or some sort of voluntary arrangement with codes, or codes of practise, or age-appropriate codes. If we go with the legislation, then it needs to be very clear and consistent with other jurisdictions, because that interoperability is going to be key, particularly if you are doing overseas enforcement.*<sup>377</sup>

As part of a discussion with the Information Commissioner about what any Government strategy to address online harms should include from a data protection perspective he advised that it must be effective, enforceable, and forward-looking and that there would be "*absolutely no point in creating legislation that is either ineffective or fails to protect people that it was designed to protect or is not practically capable of being enforced*".<sup>378</sup>

The Information Commissioner advised that legislation should not be reactive or rushed, but part of a holistic, adaptable framework that anticipates future threats and required a societal approach to address a range of harms. He advised that strategy should prioritise privacy by design, age verification, education, and strong enforcement mechanisms. It must also tackle corporate surveillance and the power imbalance between users and platforms, empowering

---

<sup>374</sup> [Written Submission – Online Harms Review – The Safeguarding Partnership Board](#)

<sup>375</sup> [Written Submission - Anonymous 7](#)

<sup>376</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.12

<sup>377</sup> [Transcript – Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.22

<sup>378</sup> [Ibid](#), p.4

individuals with greater control and accessible remedies. Some specific examples provided were:

*So looking at simple things like opt-ins rather than opt-outs would be a solution. You could also draw inspiration from the Digital Services Act and also worth looking at other programmes and codes of practice, such as the ProCoM (Project Online Content Moderatie) in the Netherlands, which facilitates the application of the E.U. (European Union) Digital Services Act to combat illegal content. That is a public-private partnership where citizens, government, and the internet sector, they collaborate and can act more efficiently where online harms and illegal content is identified. It allows for easy reporting of incidents as well as providing advice and guidance and building that knowledge capacity among providers.*<sup>379</sup>

Effective legislation must be underpinned by robust and forward-looking policy. As highlighted in a report by the Digital Futures for Children centre which specifically addresses technology facilitated CSEA, the authors emphasise the principle that policy must be adaptable and “future-proofed”, in order to anticipate emerging threats and balance immediate protections with long-term strategic resilience. Their report states that:

*This principle advocates proactive measures that enable flexibility to anticipate new threats. Such policies should balance immediate protective actions with long-term strategic adaptations to remain effective. With multiple technological innovations being actively introduced or on the horizon and multiple social, political and economic pressures on children and society, policy and practice to combat technology-facilitated CSEA [Child Sexual Exploitation and abuse] must remain fit for purpose now and in the future.*<sup>380</sup>



#### **FINDING 57**

Government of Jersey Ministers have indicated that they are introducing new legislation on online harms, however, the evidence presented to the Panel has largely focused on updates to existing laws and ongoing initiatives linked to data protection and the VAWG report. However, these efforts alone do not comprehensively address the wide-ranging nature of online harms.



#### **FINDING 58**

The Panel has heard that any new or updated legislation must be forward looking and that there should be regulatory alignment to enable cross-border enforcement and ensure child-specific protections. While Ministers value legislative autonomy, stakeholders including the NSPCC, Safeguarding Partnership Board, and Information Commissioner stressed that fragmented or reactive laws risk being ineffective.



#### **RECOMMENDATION 33**

The Government of Jersey’s online safety strategy must reflect how any legislation will address the full spectrum of digital harms and be adaptable to emerging technologies and threats.

<sup>379</sup> [Ibid](#), p. 5

<sup>380</sup> Van der Spuy, Anri et al., [Guiding principles for addressing technology facilitated child sexual exploitation and abuse](#), Digital Futures for Children Centre, December 2024, p. 4

## Clarify the role of data protection in relation to online harms

As referenced earlier, in the U.K., online harms, as defined within the context of the OSA, refer specifically to harm experienced by individuals, rather than organisations or businesses, and do not include data breaches.

Data protection supports protection from online harm by:

- Holding organisations accountable for responsible data use;
- Empowering individuals with rights to challenge misuse;
- Complementing broader online safety law;
- Enabling enforcement through regulatory bodies; and
- Providing a flexible legal framework that adapts to technological change.

However, this does not cover the full spectrum of online harms and an effective online safety strategy must clearly define the relationship between data protection and online harms. While these areas often intersect, particularly in relation to privacy, surveillance, and user rights, they are not the same and a distinction is essential.

In Jersey, data protection legislation has frequently been cited by Ministers as a mechanism for safeguarding Islanders online. As referenced in the previous section there are early plans to update the data protection law to help Islanders “*take down*” information online.

However, the Information Commissioner has cautioned against relying solely on this framework, noting that online harms legislation is not ordinarily included within a data protection enforcement regime, but rather sits within a separate legislative structure overseen by a distinct regulator. While there may be overlaps, these must be carefully managed. The Information Commissioner advised the Panel that:

*...privacy protection should sit at the core of any policy development in this area because of the quite significant overlap. I talked about corporate surveillance before, that will always be there, so privacy needs to be at the root of any legislative development in this area.*<sup>381</sup>

The Information Commissioner has also stressed the importance of maintaining alignment with the EU’s General Data Protection Regulation (GDPR). Any divergence from GDPR standards could jeopardise Jersey’s adequacy status, which is vital for the Island’s continued data flows and trade, particularly within its finance sector. Therefore, any legislative development in the online safety space must be carefully calibrated to preserve Jersey’s international standing while enhancing protections for individuals. The Panel was advised that:

*For a country such as Jersey, our adequacy is absolutely fundamental to continued dataflows and trade, and therefore critical for our finance sector, which forms the basis of our economy.*<sup>382</sup>

This was echoed by the Assistant Minister for Sustainable Economic Development who advised that:

---

<sup>381</sup> [Transcript –Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p. 22

<sup>382</sup> [Ibid](#), p.19



*A lot of work has been done to ensure that we do not disrupt the cohesion and the supportiveness of our current data protection legislation, which is built in very much with a format that has been approved by the E.U., so one of the reasons not to amend the law to providing digital rights was that.*<sup>383</sup>

The Assistant Minister for Children and Families acknowledged that legislative reform is needed to make Jersey's framework more robust and future-proof. This includes reviewing the data protection regime to ensure it can accommodate increased reporting demands and platform responsiveness, without creating unintended consequences. The Panel questioned the Minister and Assistant Minister for Children and Families about the overlap between the digital economy work and the safety of young people in online spaces and was advised:

**Assistant Minister for Children and Families:**

*Yes, there will be overlaps, but the whole thing is about ... there is 2 pieces here. First, it is about changing our legislation to make it more robust and fit for future, fit for now and fit for the future, and part of that is looking at the data protection framework, also considering any unintended consequences, because there are reporting mechanisms in the E.U. (European Union) and they have been inundated with requests. So we need to make sure, firstly, that what we have got is able to cope with the potential for those requests and equally that the platforms are going to respond to those requests. Of course there is already lots of mechanisms in place, reporting mechanisms, on all of these sites, where if you see something which is disturbing or is fraudulent activity or whatever you can self-report, and 9 times out of 10 that content will be taken down.*<sup>384</sup>

In a hearing relating to the Government's response to the VAWG Taskforce report, the Minister for Justice and Home Affairs further confirmed that policy proposals are being developed to empower Islanders to assert their online privacy rights, including takedown requests, with support from the Information Commissioner. However, questions remained about the scope of enforcement powers and the resourcing required to implement such legislation, particularly regarding which department will bear financial responsibility:

**Deputy H.M. Miles:**

*...Recommendations 10 and 11 propose giving the Information Commissioner new powers to have harmful online content removed quickly. The progress report says the scope of these powers is still under discussion. Obviously our panel have a great interest in online harms at the moment with the scrutiny that we have been doing. When will you be able to bring forward those detailed proposals covering the exact enforcement powers and the timetable?*

**The Minister for Justice and Home Affairs:**

*The officers are meeting regularly with Digital Economy colleagues to keep updated about each team's policy developments, including the proposed legislation for online platform regulation and enforcement. We have been informed that the policy proposal*

---

<sup>383</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.33

<sup>384</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.15

*developed by the Department of the Economy seeks to empower Islanders to better claim online privacy rights, such as take down requests against online platforms, if necessary, with support of the Information Commissioner. While policy is in development, it is too early to determine resourcing requirements to enforce that legislation.*

**Deputy H.M. Miles:**

*Who will fund that? Will it be Home Affairs or Sustainable Economic Development?*

**The Minister for Justice and Home Affairs:**

*The law sits with them, so one assumes it will have to sit with them as well, because it is their piece of legislation. Deputy H.M. Miles: That is potentially another hurdle then, not just the legislation, actually funding it.<sup>385</sup>*

The Panel was advised that JOIC hosted the 46<sup>th</sup> Global Privacy Assembly in Jersey in 2024. The JOIC's written submission referred to a Youth Panel consisting of students from Hautlieu School and explained that:

*The panel discussed the importance of privacy and data protection for teenagers, emphasising the need for better education and awareness, and we facilitated meetings between the panel and certain social media companies in attendance (Meta and TikTok) so that they could share their experiences directly with those operating the platforms. The panel also noted concerns about privacy settings, cyberbullying, and the impact on mental health, also stressing the need for clear, understandable privacy policies and regular updates on online safety whilst advocating for tailored approaches to social media use rather than blanket bans, ultimately calling for more inclusive conversations between law makers, regulators and the younger generation.<sup>386</sup>*

The Youth Panel's concerns reinforce the need for a strategy to facilitate the conversations that they have suggested. This is in line with the advice provided in the UNCRC's General Comment No. 25, which highlights that:

*States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children.<sup>387</sup>*

---

<sup>385</sup> [Transcript – Violence Against Women and Girls – Minister for Justice and Home Affairs - 16<sup>th</sup> July 2025](#), p.17

<sup>386</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>387</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.7-8

In summary, while data protection plays a critical role in safeguarding privacy and supporting user rights, it must be clearly outlined from the broader framework of online harms. Jersey's strategy should recognise this distinction, ensure legislative coherence, and support collaborative enforcement mechanisms that are adequately resourced and future-facing.

#### **FINDING 59**



Data protection law is critical for privacy and supporting user rights but cannot address the full spectrum of online harms. Government of Jersey Ministers have cited the importance of ensuring that Jersey's data protection laws maintain adequacy and continue to align with the EU's General Data Protection Regulation (GDPR).



#### **RECOMMENDATION 34**

Jersey must clearly distinguish between data protection and protection from other online harms in its legislative strategy, ensuring that privacy safeguards are upheld without relying solely on data protection law to address the full spectrum of online harms.

## Improve Enforcement and Accountability

An effective online safety strategy must detail how enforcement and accountability will be addressed in relation to online harms. This is essential to set out what is considered acceptable behaviour in digital environments and ensure that violations are dealt with appropriately.

General Comment No. 25 explains that children can face challenges in accessing justice relating to the digital environment. This could be due to the lack of appropriate legislation, the difficulties in obtaining evidence or identifying perpetrators, or because of a lack of knowledge (from children themselves, or their caregivers) about what abuse of their rights looks like in the digital environment. The General Comment suggests that:

*States parties should ensure that appropriate and effective remedial judicial and on-judicial mechanisms for the violations of children's rights relating to the digital environment are widely known and readily available to all children and their representatives.*<sup>388</sup>

During the public hearing in October 2024 the Minister for Sustainable Economic Development advised that the JOIC would likely lead enforcement efforts, supported by the newly established Cyber Security Centre and existing regulatory frameworks:

*We have obviously the data protection. The Office of the Information Commissioner is probably the primary route from which we can engage with the major platforms around the world and there is also the cyber security centre, which has recently been set up, and have a cyber security law and that can, as I said, speak to the side where there are particular breaches with regard to ... into their harms as well. Then the Telecommunications Law which is dealt through, I think, just through the Law Office as opposed to any other regulator and the J.C.R.A. (Jersey Competition Regulatory Authority). But I foresee that the Office of the Information Commissioner being the likely main vanguard of enforcement.*<sup>389</sup>

However, enforcement in the digital realm presents unique challenges, particularly for small jurisdictions like Jersey. The borderless nature of the internet complicates the application of local laws to entities operating abroad. The Information Commissioner explained that powers to regulate online harms must be matched by the legal and diplomatic tools necessary to enforce them across jurisdictions:

*That is not to say that our children are only at potential risk from local threat actors, but where those entities are situated in jurisdictions outside Jersey any powers given to those tasked with regulating online harms must actually be capable of enforcement i.e. they must be given the necessary legal and diplomatic tools and resources to use them effectively.*<sup>390</sup>

Without this, enforcement risks being symbolic rather than practical. This was also reflected in the submission to the Panel from Emma Martins, who said:

---

<sup>388</sup> [Ibid](#), p.8

<sup>389</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.14-15

<sup>390</sup> [Written submission – Online Harms Review – Jersey Office of the Information Commissioner](#)

*We are not a large jurisdiction. That means we have to face the reality of what enforcement outside of our borders looks like. It also means we can be nimble, and we can be responsive, but that requires us to be proactive, deliberate and thoughtful and to unite in a common aim.*<sup>391</sup>

Therefore, cross-jurisdictional cooperation is really important. The Information Commissioner also advised that the Jersey Data Protection Authority (JDPA) has an obligation to collaborate with other data protection authorities, especially when dealing with entities based in other countries. While Jersey's laws may claim extraterritorial reach, practical enforcement often depends on mutual assistance and referrals to regulators in the same jurisdiction as the offending entity:

*The J.D.P.A. has a positive obligation to engage with data protection authorities on cross-border issues, including sharing information and providing mutual assistance to other supervisory authorities with a view to ensuring that Data Protection Law is applied and enforced. An effective enforcement against entities outside of Jersey often hinges on our co-operation with other data protection authorities. How we do this depends on the issue we are dealing with largely but, for example, if an entity is based in another E.U. jurisdiction we may refer complainants to that data protection authority in that particular area, and that is because while the Data Protection (Jersey) Law may purportedly have extra territorial reach, practical enforceability again may be more easily achieved through collaboration with regulators who are in the same jurisdiction as that entity.*<sup>392</sup>

Whilst the JOIC has been suggested as a potential regulator, its current remit, which is focused on data protection, limits its capacity to enforce broader online harms legislation. In the public hearing in October 2024, the Minister for Sustainable Economic Development stated that any authority tasked with enforcement would require additional funding and resources:

*A new law that put more responsibility on to any authority, whether it is the Office of Information Commissioner or any other, would likely also need to be followed by funding to enable that enforcement to take place. When I say "yes", I do not mean yes to they are set up to do it. I mean yes, it is incumbent on the department to ensure they are in a place to be able to enforce the laws that we ask them to enforce.*<sup>393</sup>

The Information Commissioner clarified that JOIC is not currently equipped to act as the *de facto* online safety regulator, and the police are the appropriate body to report to as they have criminal investigatory powers. Any expansion of enforcement powers to the JOIC would need to be legally sound, practically enforceable across jurisdictions, and aligned with global standards.

Following the Ministerial suggestions that the JOIC would be the likely vehicle for enforcement, the Panel questioned the Information Commissioner about this idea:

**Deputy C.D. Curtis:**

---

<sup>391</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>392</sup> [Transcript –Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025,](#)

p.11

<sup>393</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024,](#) p.15

*... Given this, do you see the J.O.I.C. (Jersey Office of the Information Commissioner) acting, at least in practice, as the Island's de facto regulator for online cards?*

**Information Commissioner:**

*No, not really; not at this moment in time. I think, because the law sets out quite a strict regulatory remit for our office, which is very much based on the European General Data Protection Regulation ... we can provide advice, we can provide signposting, we receive inquiries or complaints around online harms, and of course we will deal with any regulatory issues that fall within the scope of the law. But in general terms, our remit does not currently extend to dealing with enforcing or dealing with those kind of incidents. Those other authorities, such as the police, are better to handle those matters through their criminal investigatory powers. We have an M.O.U. (memorandum of understanding) with the States of Jersey Police, which ensures that we can share relevant information with them when the time arises.<sup>394</sup>*

The Information Commissioner advised that to be effective, any enforcement framework must be:

- Legally robust and practically enforceable across borders;
- Adequately resourced in terms of funding and expertise;
- Future-facing and adaptable to technological change; and
- Consistent with global legislative frameworks to enable interoperability.<sup>395</sup>

The Panel was advised about the challenges of enforcing the law:

*The law must be capable of being enforceable. But also we could be really innovative and work together with tech companies rather than fight them. We are not going to change them. They are simply too powerful. Instead, we could work with them to make it a safer environment for children to navigate, place a responsibility on the tech companies to show young people themselves how to keep themselves [safe] online. Perhaps trial it across both Jersey and Guernsey in the first instance, and it could provide a good opportunity for Jersey to lead the way.<sup>396</sup>*

It was also noted that the JOIC is not currently resourced to deal with any increased responsibility for enforcement and it was clarified that this would require additional funding resource:

*Any addition in powers and responsibilities imposed on my office would very likely need a significant resource injection, not just in casework either, but in outreach as well is the likelihood, and expectation would be for us to increase our output in terms of guidance and education, which would be in addition to our current statutory duties.<sup>397</sup>*

---

<sup>394</sup> [Transcript –Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p. 3  
[inclusion of 'safe' was clarified during the factual checking process].

<sup>395</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>396</sup> [Transcript –Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#),

p.17

<sup>397</sup> [Ibid](#), p.14



In discussions about regulation of the online environment with the Children's Commissioner, it was suggested that working with other jurisdictions, such as the U.K. should be considered:

*Given the pace of growth and development in the online environment, this may well necessitate an online regulator in the future, or a regulation agreement with the UK. All options should be considered.*<sup>398</sup>

The Panel had queried the option of outsourcing enforcement to Ofcom in the hearing on 4<sup>th</sup> October 2024 however this was dismissed by Ministers due to concerns over accountability and capacity.<sup>399</sup>

#### **FINDING 60**



The Minister for Sustainable Economic Development has suggested that the Jersey Office of the Information Commissioner (JOIC) could potentially lead enforcement efforts for the Government's planned online safety initiatives. However, JOIC is not presently resourced to serve as the regulator, and expanding its role would necessitate substantial investment.



#### **RECOMMENDATION 35**

Before assigning enforcement responsibilities for online safety legislation, the Government of Jersey should conduct a formal capacity assessment of the Jersey Office of the Information Commissioner (JOIC) and ensure that any expansion of its role is matched with appropriate funding, staffing, and statutory authority. Additionally, the Government should consider alternative regulatory approaches, including potential partnerships or agreements with other jurisdictions.

<sup>398</sup> [Written Submission – Children's Commissioner \(follow up\) – 30<sup>th</sup> July 2025](#)

<sup>399</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.16

## Cross-Government coordination

Protecting children and young people from online harms requires a coordinated, whole-of-government approach. The Panel has been advised that various workstreams have been developed by both the Department for the Economy and the Department for Justice and Home Affairs, particularly through the response to the VAWG report.

As previously reported a cross-Ministerial group was formed in 2024. The Minister for Children and Families advised that this was to support the development of legislation and policy around online safety. Its purpose is to identify legislative gaps and ensure that relevant departments are aligned.<sup>400</sup> In respect of the group, the Minister for Education and Lifelong Learning advised the Panel that:

*I think there is an enormous amount of thought going into this. It is, I think, increasingly proactive, is the way I would say it. We met as a group. There was Ministers, myself, Economy Department, Home Affairs, the Minister for Children and Families, to talk around this topic, and we will be doing that regularly to see where we are. Because this is not just cross-government, it is across our society, which I am sure we will come to at some point.*<sup>401</sup>

The need for cross-Ministerial collaboration is further underscored by the multifaceted nature of online harms. The Minister for Sustainable Economic Development has also stressed the need to maintain a dedicated digital policy unit within government to continuously monitor and respond to the evolving digital landscape:

*I think number one is it shows the importance that you need to have a digital policy unit and maintain a digital policy unit in Jersey because it is such a unit we will be able to keep and have staff in within the Government of Jersey who are able to constantly look at the landscape. So I think that is number one that we have a digital policy unit and we need to maintain that.*<sup>402</sup>

The Government's work should be grounded in children's rights, including the principle of best interests as outlined in Article 3 of the UNCRC. The Digital Futures for Children Centre report, 'Best interests of the child in the digital environment' highlighted that:

*In sum, the best interests principle is applicable to policy making for all decisions that concern children, including business and legislative ones. This includes policies on digital services, data protection and privacy, information security, A.I. and audiovisual media as well as digital services such as those that provide or impact on public services, e-commerce, education, justice, health and other areas of public and private life.*<sup>403</sup>

---

<sup>400</sup> [Letter – Minister for Children and Families – 9<sup>th</sup> June 2025](#)

<sup>401</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p. 17

<sup>402</sup> [Transcript – Online Harms Review Public Hearing – Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025](#), p.31

<sup>403</sup> Sonia Livingstone et al., [The Best Interests of the Child in the Digital Environment](#), Digital Futures for Children Centre, March 2024, p. 7

The Children and Young People's (Jersey) Law 2022 assigns safeguarding responsibilities to key Ministers, without distinguishing between online and offline harms. The Minister for Children and Families advised that:

*Our duties and responsibilities are really covered ... the Children and Young People's (Jersey) Law 2022 sets out the key people and Ministers responsible for safeguarding children, their legal requirements, and they do not distinguish between online and offline harms. That is quite important. We have safeguarding partners and we work with the Safeguarding Partnership Board [sic], also the N.S.P.C.C. (National Society for the Prevention of Cruelty to Children), for developing and delivering children's safeguarding arrangements within their services. The Safeguarding Partnership website contains the key policies and procedures to support all those working in services to continue to safeguard. The Safeguarding Partnership also provides the key point of contacts to escalate and raise concerns for both professionals and members of the community, including children. We have got multi-agency safeguarding as well. During 2024, there was new practice guidance regarding online abuse and exploitation.<sup>404</sup>*

However, despite these arrangements, the Children's Commissioner has expressed concern that Jersey's government has yet to respond to the urgency of challenges posed through online harms, or articulate a clear plan to address them:

*I think what I would say specifically in relation to this, however, is that this is a very fast moving area and I do not believe that the Government of Jersey can afford to wait any longer to really show an understanding of the challenges that it is facing in keeping children safe online, in implementing necessary tools and initiatives, and in being clear about what the gaps and what the provisions are that it wishes to address.<sup>405</sup>*

The UNCRC's General Comment No. 25 reinforces the need for a designated government body to coordinate children's rights policy across departments and levels of government:

*To encompass the cross-cutting consequences of the digital environment for children's rights, States parties should identify a government body that is mandated to coordinate policies, guidelines and programmes relating to children's rights among central government departments and the various levels of government.<sup>406</sup>*

Emma Martins' submission echoed this and she highlighted that:

*Such a national coordination mechanism should engage with schools and the information and communications technology sector and cooperate with businesses, civil society, academia and organizations to realize children's rights in relation to the digital environment at the cross-sectoral, national, regional and local levels. It should draw on technological and other relevant expertise within and beyond government,*

---

<sup>404</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.21

<sup>405</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.13

<sup>406</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021

*as needed, and be independently evaluated for its effectiveness in meeting its obligations.*<sup>407</sup>

Currently, the Department for the Economy and the Minister for Sustainable Economic Development hold responsibility for the area of “*Digital economy*” and CYPES and the Minister for Children and Families has the formal responsibility for “*Co-ordinating policies to safeguard children and support children’s well-being*”.<sup>408</sup> Given this division, the Panel suggests that the specific considerations relating to ‘online safety’ should be led by CYPES and the Minister for Children and Families in order to ensure that the focus of the work is to prioritise child safety, rather than being secondary to broader economic objectives.

The Panel suggests that this is important to retain that focus. In reviewing the publicly available DE Strategy in 2022<sup>409</sup>, while the strategy acknowledges the importance of safeguarding, a word search reveals 20 references to “economy” and 14 to “economic,” compared to just 12 mentions of “safeguarding,” “safety,” or “safe,” suggesting a stronger emphasis on economic outcomes than child protection.

#### FINDING 61



Responsibility for the digital economy in Jersey currently sits with the Department for the Economy and the Minister for Sustainable Economic Development, while the Minister for Children and Families holds formal responsibility for coordinating policies to safeguard children and support their well-being.



#### RECOMMENDATION 36

Ministerial responsibility for online safety should be assigned to the Minister for Children and Families, in recognition of the importance of safeguarding and child protection within this policy area.

<sup>407</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>408</sup> ‘*States of Jersey Law 2005: Article 30A – Ministerial Responsibilities*’ [R.118/2024], 10<sup>th</sup> July 2024

<sup>409</sup> [Digital Education Strategy, Government of Jersey, November 2022](#)

## School curriculum and CYPES online safety policy

An effective online safety strategy must be closely aligned with the school curriculum and the CYPES online safety policy, as these frameworks shape how children and young people learn about digital risks, responsible online behaviour, and protective measures. Integration ensures consistency across education and government policy, reinforces safeguarding messages, and supports the delivery of age-appropriate, rights-based digital literacy.

Ministers have consistently emphasised the role of education in preventing online harms, a view echoed in several public submissions. However, concerns were raised about how well online safety is embedded within the current education system. Gill Hutchinson observed:

*Our education system seems to be designed for a past world that didn't function as it does today. I feel it needs to be completely shaken up, and internet knowledge, especially how social media functions, is not a nice-to-have but a vital function as important as teaching our children how to be safe in our communities and homes. The virtual reality communities are just as real to them and potentially more toxic.*<sup>410</sup>

The importance of this aspect of education was echoed in the submission from Emma Martins, who said:

*Digital literacy must be embedded into education from a very young age, with tailored age-specific content delivered by professionals. Half an hour 'online safety' or PSHE every so often is simply not good enough. It smacks of box-ticking rather than meaningful engagement. We need to influence behaviour, and impact outcomes, not just raise awareness.*<sup>411</sup>

The DE Strategy acknowledges that there was a “*thematic disunity across the Jersey school estate in how “digital” is perceived, operationalised, delivered and assessed.*”<sup>412</sup> To address this, it proposes a new Young Digital Citizen framework to standardise digital skills and competencies, including annual accreditation for pupils.

Aspects such as the use of EdTech in school and the amount of homework set to be completed on screens have been raised as points of consideration during this review. During a public hearing the Minister for Education and Lifelong Learning spoke about ensuring that there was “more co-ordination”<sup>413</sup> in setting aspects like homework online, officers acknowledged the need to understand more about the challenge of screen time balanced with equipping young people with the right skills.<sup>414</sup>

As referenced previously in the section ‘[Harm to individual health](#)’ there are various public health considerations around screen time which need consideration. Research will continue on technology that continues to develop, however, it is acknowledged that there will be challenges in keeping up with that. A report, ‘Understanding the Impacts of Generative AI Use on Children’, published by the Alan Turing Institute highlighted that:

*...there is a lack of research that considers the potential impacts of these technologies on children, even though generative AI is already being deployed within many products*

---

<sup>410</sup> [Written Submission – Online Harms Review - Gill Hutchinson](#)

<sup>411</sup> [Written Submission – Online Harms Review – Emma Martins](#)

<sup>412</sup> [Digital Education Strategy, Government of Jersey, November 2022](#), p.11

<sup>413</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.37

<sup>414</sup> [Ibid](#), p.38

*and systems that children engage with, from games to educational platforms. Children have particular needs and rights that must be accounted for when designing, developing, and rolling out new technologies, and more focus on children's rights is needed.*<sup>415</sup>

General Comment No. 25 of the UNCRC reinforces the importance of embedding digital literacy and online safety into education systems from pre-school age and outlines that the curricula should equip children with the skills to safely use digital tools, critically assess online content, and identify misinformation—especially on sensitive topics like health and human rights. They should also promote awareness of online risks such as cyberaggression and exploitation, while fostering coping strategies, data protection habits, and emotional resilience. It calls for equitable investment in infrastructure, teacher training, and evidence-based standards to ensure ethical and educational use of technology. It also recommends that teachers delivering digital literacy and sexual health education must be trained in digital safeguards.<sup>416</sup>

The Minister for Education and Lifelong Learning acknowledged the challenge of keeping pace with rapid technological change and the risks it poses to children. Budgetary pressures were also noted. The Minister acknowledged that new revenue funding would be needed to support technological advancement, describing the digital divide between schools as “*an arms race*”<sup>417</sup> but said that this was one that Jersey could keep up with.

As digital technologies evolve, including the rise of generative AI, there is a pressing need to ensure that all children are equipped with the skills and safeguards necessary to navigate the digital world safely and confidently. To support this, schools must invest in appropriate technological infrastructure and resources that enable effective and inclusive digital education.

#### FINDING 62



Digital literacy and online safety need to be embedded into education systems and keep up with technological change. The UNCRC has advised that equitable investment in infrastructure, teacher training, and evidence-based standards to ensure ethical and educational use of technology



#### RECOMMENDATION 37

The Minister for Education and Lifelong Learning should ensure that there is an equitable approach to online safety across schools and that investment is provided for technological infrastructure and resources that enable effective and inclusive digital education.

<sup>415</sup> <https://www.turing.ac.uk/research/research-projects/understanding-impacts-generative-ai-use-children> (accessed 5th August 2025)

<sup>416</sup> [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021, p.17-18

<sup>417</sup> [Transcript – Online Harms Review Public Hearing – Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025](#), p.32



## Ensure that there is support for children and young people impacted by online harm

An effective online safety strategy could also go beyond prevention and regulation and should ensure that children and young people impacted by online harm have access to timely, trauma-informed support.

The Panel questioned the Minister for Children and Families about the resources and support available to children and families affected by online harm, including cyberbullying and exposure to inappropriate content. In response, the Minister explained that support is primarily delivered through schools, which offer guidance via website content and safety-focused talks. Additional resources were highlighted on the '[Keeping your child safe online](#)' section of the gov.je website, along with support provided by the Safeguarding Partnership.

In the public hearing on 4<sup>th</sup> October 2024 the Minister for Justice and Home Affairs advised the Panel that the Government had committed to funding training through the specialist Refuge Technology-Facilitated Abuse Team in the U.K. as part of its response to the VAWG report:

*...the Government of Jersey has committed funding to invest in a comprehensive and ongoing programme of learning and development in order to strengthen the capacity of a range of services to effectively support victims and respond to online and technology facilitated abuse. This will cover both adults and children.*<sup>418</sup>

It was explained that work would begin in the first quarter of 2025 and would run for two years. Its aim was to build on-Island capacity to respond to forms of online facilitated abuse, rather than to depend on off-Island expertise. The Minister said that the training would be provided to the States of Jersey Police, school safeguarding leads, social care services for children and adults, Jersey Domestic Abuse Service, Dewberry House Sexual Assault Referral Centre and charity FREEDA (Free from Domestic Abuse).<sup>419</sup>

However, the Panel noted evidence that many young people do not report experiences of online abuse, exploitation, or privacy violations, often due to fear, stigma, or uncertainty about where to turn. The 2024 JCYPS asked respondents questions about child exploitation. It found that "Overall, considering all young people in years 8, 10 and 12 in 2024, less than half reported that they would tell someone if someone was trying to take advantage of them sexually".<sup>420</sup>

Furthermore, in relation to child criminal exploitation "Overall, 15% of males in years 8, 10 and 12 reported that they would probably or definitely not tell someone if they were offered money or gifts to do something wrong or against the law compared to 11% of females".<sup>421</sup> Whilst this does not necessarily relate to online exploitation, it highlights a broader concern about the reluctance among young people to disclose harmful experiences, including those that occur online.

In a public hearing with the Children's Commissioner, the JCYPS data was referenced:

---

<sup>418</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.3

<sup>419</sup> [Ibid](#), p.3

<sup>420</sup> [Jersey Children and Young People's Survey Report 2024](#), Statistics Jersey, 26<sup>th</sup> March 2025, p.

121

<sup>421</sup> [Ibid](#), p. 123

*I think one of the most concerning things from the children and young people survey is the number who said that they would not report to anybody attempts at either sexual or criminal exploitation. When you look at it overall, less than half of Year 8, 10 and 12 year-olds would tell anybody if there was attempts to take advantage of them sexually online, less than half. With criminal exploitation, over 15 per cent of boys say they would not tell anybody. I think that is a worrying trend, the lack of reporting. Potentially, the lack of knowledge of who to report to, who to talk to, and then all of the other pieces that go along with having an online life or existence that perhaps adults, parents, are not necessarily aware of. So I think it is a very complex problem to deal with, but the lack of reporting of potential sexual and criminal exploitation online, I think, is quite a worrying picture.*<sup>422</sup>

The Children's Commissioner's written submission noted the importance of clear reporting mechanisms:

*Children should have access to reporting mechanisms when they have experienced online abuse, exploitation or violation of their privacy. This includes the ability to seek redress through complaints mechanisms, legal avenues, and support services. Remedies should be child-friendly and accessible, ensuring that children can easily report harm and have their cases addressed promptly.*<sup>423</sup>

Without clear, accessible pathways for help and redress, harmful experiences can escalate and leave lasting impacts. Embedding support services, mental health resources, and community education into Jersey's online safety framework is essential to protect vulnerable users and promote digital wellbeing.

In the [written submission](#) to the Panel from the Safeguarding Partnership, they highlighted that following the joint conference with the NSPCC (in November 2024) attendees had provided ideas about priority areas for Jersey. One of the main areas described was around support systems, under that heading included:

- **For Children & Parents:** Strengthening trauma-informed services and creating clearer support pathways.
- **For Professionals:** Equipping teachers, youth workers, social workers and agencies with tools for effective intervention.
- **Through Collaboration:** Enhancing multi-agency frameworks to ensure shared accountability and streamlined support services<sup>424</sup>



### FINDING 63

Data from the Jersey Children and Young People's Survey suggests that some young people are hesitant to report experiences of criminal or sexual exploitation. While not all such harm occurs online, the data underscores the importance of establishing clear, accessible reporting pathways and support systems to safeguard children in digital spaces.



### RECOMMENDATION 38

The Government should establish clear, child-friendly reporting pathways for online harm, supported by community learning initiatives that empower children,

<sup>422</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.8

<sup>423</sup> [Written Submission – Children's Commissioner for Jersey](#)

<sup>424</sup> [Written Submission – Online Harms Review – The Safeguarding Partnership Board](#)

parents, and professionals to recognise and respond to exploitation. A simple, accessible system for Islanders to report harmful online content, accompanied by clear guidance on what to report, where to report it, and who handles it, should be developed.

## Engage businesses and digital platforms

An effective online safety strategy for Jersey must include meaningful engagement with businesses and digital platforms. These entities play a central role in shaping the digital environments that children and young people interact with daily. As such, they must be active partners in efforts to protect users and uphold digital rights.

### International obligations: General Comment 25

The United Nations Committee on the Rights of the Child, in General Comment No. 25 (2021), makes clear that States have a duty to ensure that businesses respect children's rights in the digital environment. This includes requiring companies to conduct child rights due diligence, assess risks, and take proactive steps to prevent harm. Jersey's online safety strategy must reflect these obligations by setting clear expectations for local and international tech companies operating within its jurisdiction.

### Collaboration

The Panel was advised in May 2025 that the JOIC had already begun discussions with the Children's Commissioner, Government of Jersey, and NSPCC Jersey to develop a guidance note and checklist for technology companies.<sup>425</sup> This initiative aims to support developers of websites and applications that may be accessed by children, ensuring that safety and privacy are embedded from the outset.

When asked what single change could most improve online safety for children in Jersey, the Information Commissioner emphasised the importance of collaboration over confrontation:

*I think working collaboratively with the tech companies and social media platforms to help young people understand how to keep themselves safe online. We spend a lot of time as regulators and as jurisdictions fighting these big tech companies and it is futile. And I think you would agree to that, because you are not going to win. They are simply too powerful, too big, and hold a lot of power in terms of market values and whatever. Are we going to be able to change it? No. So, rather than fight them, let us, for want of a better description, get into bed with them and let us get them on side and work with them.*<sup>426</sup>

This pragmatic approach recognises the immense influence and resources of global tech platforms. By fostering partnerships, Jersey can help young people better understand how to stay safe online while encouraging platforms to adopt child-friendly design and moderation practices.

### Preventing Regulatory Evasion

The Panel was curious to understand whether concerns had been raised about Jersey potentially being used as a jurisdiction to evade online safety regulations enforced elsewhere. The Panel questioned whether the Government had assessed this risk, and the Minister for Sustainable Economic Development acknowledged that while no formal assessment had been made, it was a concern for consideration:

---

<sup>425</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>426</sup> [Transcript – Online Harms Review Public Hearing – Information Commissioner – 7<sup>th</sup> July 2025](#), p.19

**Deputy H.M. Miles:**

*... It is just questions around whether Government has assessed whether there is a risk to Jersey being used as a jurisdiction to avoid the online safety regulations elsewhere and how that has been taken into account with the policy development.*

**The Minister for Sustainable Economic Development:**

*I do not believe we have made that assessment yet, but it is something that I am personally aware of and would absolutely not want to see happen. This is not a place where we would want to have people using in any way the Island for those purposes, so again, that is something that we should make sure is dealt with in the law and you do that by making it clear that in Jersey if you are doing X or Y, you will be prosecuted. You will be caught and prosecuted and that is how you do that. So, that is why it is really important that we do have these laws in place. I think it is also important that Ofcom itself does not do criminal prosecutions and could not in Jersey particularly either, so from that perspective it would not be convictions against someone.<sup>427</sup>*

This underscores the need for robust legislation that makes clear Jersey's commitment to online safety and ensuring it does not become a jurisdiction used for digital regulatory avoidance.

The Government has confirmed that regular consultation with industry stakeholders has taken place in the development of Jersey's Digital Economy Strategy. The Minister for Sustainable Economic Development opined that online safety regulations would not negatively impact legitimate local businesses, but he acknowledged the importance of remaining vigilant and responsive to emerging risks to ensure that did not happen in Jersey in the future.<sup>428</sup>

Balancing innovation and protection

During the hearing with the Minister for Children and Families the Panel asked if there were potential conflicts of interest between business innovation and protecting children online:

**Deputy B.B. de S.V.M. Porée:**

*Do you feel there could possibly be there a conflict of interest between the interests of businesses, the developing of the new technology, as well as protecting children and users?*

**Head of Governance and Digital, C.Y.P.E.S.:**

*I think there are lots of different parties around the table and therefore there is a wide enough scope, enough people to be able to make sure that there is no conflict of interest.*

**Deputy B.B. de S.V.M. Porée:**

*So you agree that there will possibly be conflicts of interest?*

**Head of Governance and Digital, C.Y.P.E.S.:**

---

<sup>427</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.34-35

<sup>428</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.36

*Potentially, but I do not think that there will be any difficulties with that.*<sup>429</sup>

## Other jurisdictions

Across the world, governments and organisations are grappling with how best to safeguard children in digital environments. While approaches vary, several emerging practices and challenges offer valuable lessons for Jersey. The Panel was informed that other Commonwealth jurisdictions have the most comparable legislative frameworks to Jersey, and that these are reviewed to help design any new legislation locally.<sup>430</sup>

As part of the review, the Panel heard from multiple sources that the action Jersey takes to prevent online harms impacting Islanders requires a proportionate and locally informed response. The Information Commissioner advised caution when looking to other, larger, jurisdictions:

*There is clear temptation for small jurisdiction to adopt policy frameworks from larger countries as a template, but doing so without adaptation to local context can be ineffective and unsustainable.*<sup>431</sup>

He explained that this was because the volume and nature of online harms may differ and that:

*What may be suitable and necessary in other jurisdictions may not be suitable or necessary to the same extent in Jersey and it is important to have a very clear understanding of what is (or is not) actually affecting the island's children so that any policy or legislation can be tailored and effective whilst also representing a proportionate response to identified risks both here, and internationally.*<sup>432</sup>

However, there are voices of concern about international regulatory fragmentation, where differing national laws and enforcement standards create loopholes and inconsistencies. This can undermine efforts to establish universal safeguards and allow companies to exploit jurisdictional gaps.<sup>433</sup>

For example, research has shown that children in the Global South often receive weaker protections from tech companies, especially when content or safety tools are not available in local languages.<sup>434</sup> Meanwhile, France has taken steps to introduce mandatory age verification to access adult content on platforms and has trailed restrictions on mobile phone use in schools. In regions like California, data protection frameworks still struggle to fully align with the best interests of the child in digital spaces.<sup>435</sup>

Australia's regulatory stance continues to evolve, particularly around platform bans and enforcement mechanisms. However, some experts caution that such measures may be

---

<sup>429</sup> [Transcript - Online Harms Review Public Hearing – Minister for Children and Families – 23<sup>rd</sup> May 2025](#), p.16-17

<sup>430</sup> [Transcript – Standalone Hearing re Online Safety for Children in Jersey - 4<sup>th</sup> October 2024](#), p.33

<sup>431</sup> [Written Submission – Jersey Office of the Information Commissioner – 14<sup>th</sup> May 2025](#)

<sup>432</sup> [Ibid](#)

<sup>433</sup> 'Towards Digital Safety by Design for children', OECD Digital Economy Papers, June 2024 (No.363), p.5

<sup>434</sup> 'The children's rights-by-design standard for data use by tech companies', P. Hartung, UNICEF, Good Governance of Children's Data project, November 2020, p. 4

<sup>435</sup> Sonia Livingstone et al., [The Best Interests of the Child in the Digital Environment](#), Digital Futures for Children Centre, March 2024, p. 19



difficult to enforce, risk infringing on rights, and can be easily bypassed by tech-savvy children or adults. The focus, instead, is shifting toward making digital experiences safer through shared responsibility among platforms, regulators, and caregivers.

The Panel sought the Children's Commissioner's view on whether children in Jersey should be prohibited from having social media accounts. She responded that, from a rights-based perspective, such a restriction would not achieve an appropriate balance, as it would deny children access to valuable digital experiences. She stated:

*Given children's capacity to bypass, and we know we have seen it from the children and young people survey, all kinds of controls and safety measures and access, etc cetera, I think it will be very difficult to either monitor or police. I know that that is a route that the Australian Government has gone and but I think we are yet waiting to see exactly how that is going to be implemented, policed, controlled, because I think that is not yet clear. I think the other issue that we will have and we will always have for a minority is that children will simply be given access by adults. So I am not sure of how effective a ban on social media platforms would be for children and how one would separate that out completely for access for adults.<sup>436</sup>*

---

<sup>436</sup> [Transcript – Online Harms Review Public Hearing - Children's Commissioner for Jersey – 16<sup>th</sup> July 2025](#), p.16

## **Conclusion**

This review has focused on online harms, recognising that concepts of harm and safety are highly context dependent and that online access does not inherently equate to risk.

While the benefits of digital engagement are clear, Jersey's current protections for children fall short of international standards, and further work is urgently needed to close gaps in areas such as age verification, data protection, and platform accountability. Drawing parallels with offline safety expectations, the Panel highlights the need for enforceable, rights-respecting structures that safeguard children without compromising freedom of expression or access to information.

The decision to pursue bespoke legislation rather than adopt the U.K.'s Online Safety Act must be supported by evidence and strategic coordination to avoid regulatory fragmentation.

Embedding child rights into digital governance, enhancing cross-Government collaboration, and aligning educational policies with safe technology use will be essential for Jersey to build a resilient and future-facing framework that protects children and promotes their digital wellbeing.

The Panel has made a total of 63 findings and 38 recommendations in this report, which are all intended as a call to action for Government. From these, 6 key findings and 5 key recommendations have been highlighted for particular consideration.

The Panel hopes that the findings of this review will be of interest to the public and that the Recommendations will be carefully considered and implemented by Government.

## **Appendix 1**

### **Panel membership**

The Panel comprised of the following States Members:



Deputy Catherine  
Curtis (Chair)



Connétable Mark  
Labey (Vice-Chair)



Deputy Beatriz Porée  
(resigned from the  
Panel on 21<sup>st</sup>  
October 2025)



Deputy Helen Miles

### **Terms of Reference**

1. To examine and establish the protection in place for children in Jersey from online harms, to include consideration of:
  - (a) Legislation;
  - (b) Regulation;
  - (c) Government policy;
  - (d) The role of internet service providers and technology;
  - (e) The role of social media platforms, content providers and content creators; and
  - (f) The role of education, family, and culture.
2. To establish what is considered good practice, and strong safeguarding, for children within online environments and a digital world and consider this in the context of Jersey's position.

### **Evidence considered**

#### **Public Hearings**

The Panel held public hearings with the following witnesses during the Review:

- The Minister for Education and Lifelong Learning – 16<sup>th</sup> May 2025;
- The Minister for Sustainable Economic Development and the Assistant Minister for Sustainable Economic Development – 16<sup>th</sup> May 2025;
- The Minister for Children and Families and the Assistant Minister for Children and Families – 23<sup>rd</sup> May 2025;
- The Minister for Justice and Home Affairs – 23<sup>rd</sup> May 2025;
- The Information Commissioner for Jersey – 7<sup>th</sup> July 2025; and

- The Children's Commissioner for Jersey – 16<sup>th</sup> July 2025.

The Panel also held a public hearing with the Minister for Children and Families, Minister for Justice and Home Affairs and the Minister for Sustainable Economic Development in October 2024, prior to the start of the review, which has formed part of the evidence and information used in this report.

Transcripts of the hearings are available [here](#).

### **Official Correspondence**

The Panel wrote to the following Ministers and received responses to written questions from:

- The Minister for Education and Lifelong Learning;
- The Minister for Sustainable Economic Development;
- The Minister for Children and Families;
- The Minister for Justice and Home Affairs

### **Written Submissions**

Direct requests for written submissions were sent to a variety of stakeholders. Responses were received from the following:

- The Children's Commissioner for Jersey
- Jersey Office of the Information Commissioner
- Public Health, Jersey
- Safeguarding Partnership Board
- NSPCC Jersey
- JT
- Tik Tok

There was a public call for evidence and

- Highlands College
- Cardin Pasturel
- Jon Tarrant
- Emma Martins
- Dr. Chis Edmond
- Victoria O'Neil
- Gill Hutchinson
- Smartphone Free Childhood Jersey
- 19 submissions from members of the public who asked to be anonymous

The Panel also received a number of confidential submissions that we did not receive permission to publish.

To view all the submissions, responses to written questions please visit the review page on the States Assembly website ([here](#)).

### **Bibliography of sources used for desktop research:**

- [General comment No. 25 \(2021\) on children's rights in relation to the digital environment](#), Committee on the Rights of the Child, United Nations Convention on the Rights of the Child, 2<sup>nd</sup> March 2021
- [Children in the Digital Environment: Revised Typology of Risks](#), OECD Digital Economy Papers, January 2021, No. 302
- [The children's rights-by-design standard for data use by tech companies](#), P. Hartung, UNICEF, Good Governance of Children's Data project, November 2020
- [Statistics briefing: online harm and abuse](#), NSPCC, October 2024
- [Evidence Review on Online Risks to Children: Executive Summary](#), Dr. J. Bryce, et al., NSPCC, November 2023
- [Toolkit for Digital Safety Design Interventions: Typology of Online Harms](#), World Economic Forum, August 2023
- [Multi-Agency Child Sexual Abuse and Exploitation Strategy](#), Safeguarding Partnership Board, July 2022
- [Impact of regulation on children's digital lives](#), S. Wood, Digital Futures for Children Centre, May 2024
- [Towards Digital Safety by Design for children](#), OECD Digital Economy Papers, June 2024 (No.363)
- [Smartphone policies in schools: What does the evidence say?](#), Miriam Rahali et al., Digital Futures for Children Centre, September 2024
- [The Best Interests of the Child in the Digital Environment](#), Sonia Livingstone et al., Digital Futures for Children Centre, March 2024
- [Digital Education Strategy](#), Government of Jersey, October 2022
- [Children and the Digital World](#), Government of Jersey, May 2022
- [CYPES Counter Bullying Policy](#), Government of Jersey, March 2019
- [CYPES Online Safety Policy](#), Government of Jersey, August 2021
- [Keeping Children Safe in Education Policy](#), Government of Jersey, September 2024
- [Children, Young People and Families' Plan for 2024-2027](#), Government of Jersey, May 2024
- [Jersey Children and Young People's Survey Report 2024](#), Statistics Jersey, 26<sup>th</sup> March 2025

### **Review costs**

The costs of this review totalled £1,439.00 for advertising, engagement, and public hearing transcription costs.

## What is Scrutiny?

Scrutiny panels and the Public Accounts Committee (PAC) work on behalf of the States Assembly (Jersey's parliament). Parliamentary Scrutiny examines and investigates the work of the Government, holding ministers to account for their decisions and actions. They do this by reviewing and publishing reports on a number of areas:

- Government policy;
- new laws and changes to existing laws;
- work and expenditure of the Government;
- issues of public importance.

This helps improve government policies, legislation and public services. If changes are suggested, Scrutiny helps to make sure that the changes are fit for purpose and justified. The Children Education and Home Affairs Scrutiny Panel reviews policy and legislation related to the topics of children, young people, education and home affairs. It focuses mainly on the work of the Minister for Children and Families, the Minister for Education and Lifelong Learning, and the Minister for Justice and Home Affairs. To learn more about the Panel's work please click [here](#).





States Greffe | Morier House | Halkett Place | St Helier | Jersey | JE1 1DD  
T: +44 (0) 1534 441 020 | E: [statesgreffe@gov.je](mailto:statesgreffe@gov.je) | W: [Statesassembly.gov.je](http://Statesassembly.gov.je)

