JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

Deputy Catherine Curtis
Chair, Children, Education and Home Affairs Scrutiny Panel
Scrutiny Office
States Greffe
Morier House
St Helier
Jersey
JE1 1DD

By Post & Email: k.decarteret@gov.je

14 May 2025

Dear Deputy Curtis

Children, Education and Home Affairs Scrutiny Panel review: "What protection do children in Jersey have from online harms?"

Thank you for the opportunity to engage in your panel's review, as outlined in Ms De Carteret's email dated 23 March 2025. I am grateful for your officer affording us the ability to reply slightly outside the anticipated timeframe.

The Jersey Office of the Information Commissioner (**JOIC**) has, as one of its strategic goals, a key strategic outcome of *"Putting Children First"*. This means that a key area of focus for this office is on protecting children's data and fostering an island culture where privacy is understood and respected, including by way of raising awareness among children about their data protection rights, the importance of protecting their personal information and giving them to tools to help them do this. Our long-term vision is to create a culture in Jersey where *"Privacy Becomes Instinctive"* with all islanders (including children) taking a proactive approach to embed such protection through their daily activities.

As you may be aware, we have engaged directly with the Minister for Sustainable Economic Development (and his Assistant Minister and policy advisers) over many months about this topic (including on proposed legislative models) but we are grateful for the opportunity to provide responses to the questions you have directly raised with us and in so doing, hope to outline the capabilities and limitations of existing legislation, highlight certain challenges of importing regulatory models from other jurisdictions and, respectfully, offer suggestions for a pragmatic and Jersey-specific way forward.

We have generally limited our comments to areas which interact with our data protection remit and have not commented on topics such as health-related harms or the efficacy of the measures proposed, except where it is relevant to data protection.

That is not to say that we have disregarded them, but there are others who have provided responses best qualified to opine on those particular aspects.

Your questions

How data protection law applies to online content moderation processes in Jersey and the rest of the world

1. Online content moderation by platforms will ordinarily involve the processing of personal data and in those circumstances will be subject to data protection laws, including in Jersey under the Data Protection (Jersey) Law 2018 (**DPJL 2018**) and in many other jurisdictions worldwide. These laws apply to online content moderation processes when personal data is involved, ensuring that any processing is lawful, fair and transparent by the platform. It may involve the content itself, but also associated data such as usernames, IP addresses, behavioural data etc. The DPJL 2018 applies to both controllers and processors established in Jersey and may include those located outside the island if they fulfil certain establishment criteria[1]. This means that content moderation systems used by large global platforms may fall within scope subject to fulfilling that establishment criteria and where they do, they must also comply with core data protection principles of lawfulness, fairness, transparency, purpose limitation and data minimisation.

The extent of the powers provided under the Data Protection Authority (Jersey) Law 2018 in relation to protection from online harms

2. When it came into force on 5 May 2018, the Data Protection Authority (Jersey) Law 2018 (**DPAJL 2018**) established an up-to-date framework for Jersey's data protection regime, aligning closely to the General Data Protection Regulation (**GDPR**) which was crucial for ensuring that Jersey maintained its adequacy status with the European Commission. It also established the Jersey Data Protection Authority (**JDPA**) as the island's independent supervisory authority with responsibility for data protection tasked with ensuring compliance with the DPJL 2018 by public bodies and private entities alike.

3. 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

[1] Art.4(2) of the DPJL 2018

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.

4. In terms of the JDPA's powers, it has the power *inter alia* to:

    a. Investigate complaints from data subjects when those individuals have concerns that a data controller has or will contravene the DPJL 2018

    b. Initiate formal inquiries either of its own initiative or where matters have come to its attention due to a whistleblower or during another investigative process

    c. Impose a variety of orders against a data controller/processor including deletion of material, seizing of equipment, issuing of stop processing orders, reprimands and administrative fines

    d. Raise public awareness through education, outreach and guidance

    e. Work with regulatory bodies in other jurisdictions on cross-border matters.

5. These powers are targeted at addressing data protection related harms such as tracking, targeting, lack of transparency and unlawful processing by online platforms rather than broader harms like dealing with harmful or illegal content or cyber bullying by online platform users.

6. We mention this because it is important to recognise that the law does not apply to individuals who process personal data in the context of a purely personal or household activity. This is known as the domestic purposes exemption and individuals who process personal data for a purely personal activity (such as uploading photos, comments or videos to social media platforms) are not ordinarily subject to data protection law. As a result, the JDPA has no legal authority to regulate or sanction individuals acting in a private capacity even if the content they upload contributes to online harm. The law distinguishes between the responsibilities of data controllers (social media platforms usually expressly stating 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) and the freedoms of private individuals. Accordingly, this limits the role data protection law can play in addressing person-to-person online harm or harmful user behaviour not mediated through a controller's own processing systems. This separation is consistent with supervisory authorities in other jurisdictions including the UK where the UK's Information Commissioner does not enforce against individuals.

7. We have noted in certain of the responses (and as part of the scrutiny review more broadly) a suggestion that it may be prudent to adopt a regulatory framework akin to that which has emerged in either the UK or Australia citing as a positive that alignment of regulatory requirements *"would likely offer the best form of online safety protection for children in Jersey"*[2]. 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 for the following reasons:

    a. The volume and nature of online harms may differ. The most recent population estimate issued by the UK's office for national statistics suggested a population of 68,265,200[3] for the UK. In Australia it is said to be 27,309,396[4]. In comparison, Jersey's is 103,650[5]. Those larger jurisdictions naturally attract more aggressive enforcement needs and higher incidences of online harms given volumes of potential platform users, but Jersey's smaller population and digital footprint may experience different types of risk and harms, including more community driven (e.g. bullying in local networks) which require tailored, proportionate responses. 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.

    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. This is very important because powers that may appear on paper to be suitable and workable, may be quite different in practice, with those cross-border provisions not actionable in reality. A good example of this issue in practice relates to the extra territoriality provisions that are built into the GDPR and the steps taken by certain Data Protection Authorities (DPAs) against the non-EU based ClearviewAI. Despite clear findings by the relevant EU DPAs and the imposition of significant fines about its processing activity, ClearviewAI has refused to comply with the DPAs on the basis that it does not operate within the EU and is not therefore subject to the jurisdiction of the EU DPAs.

---

[2] NSPCC Jersey briefing dated February 2025

[3] https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/timeseries/ukpop/pop

[4] https://www.abs.gov.au/statistics/people/population

[5] https://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/Jersey%20population%20and%20migration%20statistics%202023.pdf

This is highly relevant in the context of an online harms framework as even if any law claimed jurisdiction over foreign entities that target or monitor individuals in Jersey, the ability to effectively enforce will depend on the entity either having a presence in the Island or will rely on the cooperation of foreign courts or mirror authorities in those jurisdictions.

The JDPA has a positive obligation to engage with DPAs on cross-border issues *"including sharing information and providing mutual assistance to, other supervisory authorities with a view to ensuring the Data Protection Law is applied and enforced"*[6] and effective enforcement against entities outside Jersey often hinges on our cooperation with other DPAs. How we do this depends on the issue we are dealing with but, for example, if an entity is based in another EU jurisdiction we may refer complainants to the DPA in that area. This is because whilst the DPJL 2018 may purportedly have extra-territorial reach, practical enforceability may be more easily achieved through collaboration with regulators in the same jurisdiction as the entity.

Our ability to ensure safety for the island's residents (particularly our children) relies not only on the strength of any domestic legislation, but also on the relationships we have with regulators in other jurisdictions.

b. The scale and resourcing for Jersey compared with those larger jurisdictions are often not comparable in that regulatory models. Legal and regulatory models such as those in the UK and Australia are (presumably) built on a premise of large-scale enforcement bodies with extensive legal, technical and financial resources available at their disposal. Calls to simply replicate those models in Jersey must be approached with a certain degree of caution. Those regimes, though apparently robust on paper, may not be so in practice and careful thought would need to be given whether those frameworks actually work from a Jersey perspective as Jersey's size and legal framework differs from both the UK and Australia and simply importing legislation wholesale creates a risk of imposing an overly burdensome system that cannot be properly resourced, enforced or justified given local realities.

   The JDPA's funded position is very different to the two regulators in the jurisdictions cited as comparators. Ofcom is the regulatory body with oversight for the UK OSA and had an income of £190,151,000 for the y/e March 2024[7].

[6] Art.11(h) DPAJL 2018 and see also Art.15 DPAJL 2018.
[7] https://www.ofcom.org.uk/siteassets/resources/documents/about-ofcom/how-ofcom-is-run/annual-reports/plans-and-financial-reporting/annual-reports/annual-report-2023-24/ofcom-annual-report-and-accounts-2023-2024.pdf?v=384868

In Australia, responsibility falls to the eSafety Commissioner (which is funded by Australian Communications and Media Authority) and who saw its funding increase in 2023 to $42.5m[8] (equivalent to £20,626,000) against a background of concerns that the office was insufficiently resourced to carry out its activities under the Aus OSA. This is mentioned because Jersey's regulatory environment is considerably smaller and more limited in capacity. Mirroring the two frameworks mentioned would likely outstrip available resources and enforcement capabilities of the JDPA.

c. Early implementation challenges in both the UK and Australia. It is important to note that both the UK OSA and Aus OSA are still in very early phases of implementation and the regimes have not been thoroughly tested including in terms of the ability and ease of enforceability against large, global technology companies and this by regulators that have the resources available to pursue such avenues. Any cross-border legal enforcement is complex and resource intensive if pursued, both in terms of human and financial resources. The first legal challenge of Judicial Review of the UK OSA has recently been announced by Wikimedia Foundation (about categorisation rules that set out how Ofcom will decide which websites have to follow the most stringent duties[9]) and there are legitimate questions that have been raised about whether the regulator has sufficient powers to enforce the law and whether it captures the platforms actually of concern. Uncertainty remains about how these new regimes interact with the concepts of freedom of expression, platform responsibility and user rights.

d. Where any function would sit. As noted elsewhere in this note, online harms legislation is not ordinarily included within a data protection framework or enforcement regime but rather as a separate piece of legislation overseen by a different regulator. Careful thought would need to be given about who is best placed to oversee any regulatory regime and how to legislate as would the impact of this on our data protection adequacy status. The JDPA are open to consultative discussions around the oversight of online harms legislation with other relevant stakeholders including consideration of all implications.

[8] https://minister.infrastructure.gov.au/rowland/media-release/record-investment-improve-safety-australians-online
[9] https://www.bbc.com/news/articles/c62j2gr8866o

For the period 2018-2024 in Jersey, how many complaints have been made to the Data Protection Authority (as per Part 4 of the Data Protection Authority (Jersey) Law 2018) and how many inquiries have been undertaken

8. Information about the JDPA's regulatory activity is regularly published in its Annual Reports, including its case-handling data and information about the JDPA's enforcement activity can be found in our Regulatory Action and Enforcement Policy[10].

Year	Number of complaints received (not all investigated) (Art.19 DPAJL 2018)	Number of formal Investigations (Art.20 DPAJL 2018)		Number of formal Inquiries (Art.21 DPAJL 2018)
		Breach Determined	No Breach Determined	
2022	58	6	11	4
2023	80	15	5	4
2024	82	22	3	4

9. If the question was to ascertain how many complaints have been made about online harms (such as exposure to harmful content, cyber bullying, online exploitation or grooming) the answer to that is nil. We note the submission of the Children's Commissioner (specifically para.21) and wonder if the States of Jersey Police have been able to produce any similar statistics about reports made to them about such matters and, if so, what action was taken to deal with them?

10. Similarly, this office has received very few complaints about social media platforms generally and none relating to any refusal to act on erasure requests or similar. This information and certain other related information has already been communicated to Deputy Morel's team when previously requested.

How rapidly advancing technology increases privacy risks specifically for children and young people

11. It is right to acknowledge that rapid technological advancements have increased privacy risks for children and young people in several ways.

    a. Data collection: Many online services (including gaming platforms and certain interactive toys with internet connectivity) often collect vast amounts of personal data (often without clear, or lawful consent). This can lead to potential misuse of information.

[10] https://jerseyoic.org/media/l5sfz1s0/joic-regulatory-action-and-enforcement-policy.pdf

b. Profiling and targeted advertising: As a result of data collected by the systems (either that proactively provided by the child or because of the use of the platform) children may be subjected to profiling, resulting in targeted advertising that can influence their behaviour and choices.

c. Lack of understanding: Children may not fully understand privacy notices (that ought to contain information about how information is collected and used) or the implications of sharing personal information online. Similarly, parents may not have a fulsome understanding of the platforms used by their children or know what information is being provided by their children and/or collected by the platforms themselves.

d. Exposure to inappropriate content: Algorithms may inadvertently expose children to harmful or inappropriate content. Certain platforms allow direct communication by users and children may be at risk of interaction with users who may not be who the children think they are.

Details about any education or engagement work undertaken by the JOIC with the public about their rights relating to online privacy risks for their personal data

12. Part 2 Art.11(d) of the DPAJL 2018 states one of the functions of the JDPA is to *'promote public awareness, risks, rules, safeguards and rights in relation to processing especially in relation to children'* and in line with our strategic outcome to *'protect our future generations by putting children and young people first'* the learning outcomes of our young persons' programme for 2024 were:

    a. To raise awareness of our role and obligations and how they can support individuals in protecting their personal information and privacy rights.
    b. To raise individuals' awareness of their privacy rights.
    c. To increase knowledge of key privacy issues and promote good privacy behaviours for privacy to become instinctive.
    d. To provide practical, actionable insights to help individuals confidently protect their personal information.

13. 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'*. We delivered the following:

    a. 10 Privacy Awareness assemblies for Key Stage 2 students (7-11 years old)

b. 28 sessions highlighting 'The Importance of Protecting Personal Information' and Awareness of Digital Footprint, for Key Stage 3 students (11-12 years old)
c. 19 sessions highlighting 'Understanding Information Rights' for students in years 8 and 9 (12-14 years old)
d. 25 sessions about 'Data Protection responsibilities in the Workplace and Data Protection Principles' for students at Key Stages 4 and 5 (14 – 18 years old) who are undertaking industry work placements
e. Three 'Privacy Debate' sessions allowing students at Key Stage 4 (15-16 years old) to research, reason and deliver arguments around privacy themes
f. Three bespoke 'Courtroom Challenges' bringing data protection law to life for students at Key Stage 5 (16-18 years old)

14. 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. Accordingly, the aim of our measured programme of engagement activities and educational events for community members of all ages from sports clubs, to schools, youth clubs, cultural associations and volunteering groups was to educate participants about privacy and data protection matters and further embed our vision to create an Island culture whereby privacy is instinctive.

15. Our Community Outreach team also attended Island events throughout 2024 accompanied by our privacy superhero life-size characters enabling families to engage with our educational activities and learn about the importance of protecting personal information. The largest of these was the Government of Jersey's Children's Day for 2024 which attracted more than 10,000 members of Jersey's community. Other activity included a presence at a Jersey adventure park, Jersey Library's Summer Reading Challenge and a privacy themed bear hunt, as well as a privacy trail through St Helier. These sessions provided the opportunity for us to hear directly from Jersey's community about any challenges they face related to data protection, levels of understanding of the law and how it helps to protect and empower them, as well as common misconceptions.

16. We also collaborate with other agencies where appropriate for example the Fraud Prevention Forum and Jersey Cyber Security Centre, providing targeted awareness campaigns.

17. From January 2025 we will focus our energies with our young persons' programme with students aged 11 to 18, only. This is in response to session survey feedback, our own reflection, as well as teacher reflections that stated the school curriculum covers what we were able to deliver during primary school assemblies and therefore our efforts could be

best utilised with Key Stage 3, 4 and 5 (ages 11 to 18). Whilst we recognise many behaviours regarding privacy and technology could be learned at an early age, the current PSHE curriculum covers what is appropriate for this age group and we found we were unable to add any value to what was being delivered by teaching professionals.

18. For your information, we are currently engaged in discussions with both the Children's Commissioner, Government of Jersey and the NSPCC Jersey about the development of a guidance note/checklist for local technology companies engaged in the development of applications and websites that may be accessed/used by children. Those discussions are at an early stage but the first step will be the holding focus groups with the Children's Council (made up of representatives from each of the island's schools) so we can gain a fulsome understanding from children about what technology they are using and the issues they encounter, so that any guidance we produce is reflective of reality and meaningful. Those group meetings are due to take place in November 2025, and we are also meeting with the Youth Panel that is supported by the Children's Commissioner on 15 May 2025, to ask initial questions about the type of platforms accessed by children and what their experiences of those platforms are.

General observations

We have considered all the reviews provided so far and those are published on your website[11]. Whilst not the focus of your questions to this office, we would also like to offer our thoughts on responses focused on restriction of access to smartphones (either generally for those under the age of 16 or specifically in the school setting) as a means of protecting children from online harms such as cyberbullying, exposure to inappropriate content and reducing excessive screen time. Whilst fully understanding the suggestion that smartphone bans (particularly) in schools, will help to reduce the risk of exposure to these issues, we are now operating in a world where technology is so embedded in our daily lives that from a young age, children are reliant on technology as part of their education. 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.

Indeed, as Jo Terry-Marchant notes in her submission, *"We are experiencing a 'new' normal"* and what is required is a pragmatic, multi-disciplinary approach that involves education at all levels (children, parents etc) and which also equips children with the skills they need to successfully and safely navigate the world in which they live, and will need to navigate as adults. We note, with interest, the comments made by Public Health about certain jurisdictions complementing "regulation with strong educational approaches and educational support" and that the jurisdictions referred to *"have developed national campaigns to support parents,*

[11] https://statesassembly.je/search?documentType=Submissions&panel=200002

teachers and young people in navigating digital environments safely and mindfully" and we concur with Public Health's suggestion that *"fully addressing the issue will require a co-ordinated, whole society approach".*

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. Could potential restrictions cause unintended consequences and potential risk of more serious harm?

As you may be aware, this office hosted the 46th Global Privacy Assembly in Jersey last year and one of our panel sessions was a Youth Panel consisting of students from Hautlieu School. Whilst the focus of their session was on privacy, social media featured heavily in their discussions, statistics highlighting that 80% of children in the Western world have a digital footprint by age two, and 46% of teenagers are almost constantly online. 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.

Concluding remarks

The issues relating to online harms are complex and wide-ranging and we welcome further engagement as discussions in this important area progress. Specifically, 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. Please do not hesitate to contact us should you have any queries regarding our response at consultation@jerseyoic.org.

Yours sincerely

Paul Vane
Information Commissioner