Minister for Education
and Lifelong Learning

Government of JERSEY

Union Street | St Helier
Jersey | JE2 3DN

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

Sent by email only

10 March 2025

Dear Chair,

Scrutiny Review: What protection do children in Jersey have from online harms

Thank you for your letter of 24th February asking a range of questions on the above topic.

Please see the below answers to your questions and do not hesitate to contact me again if you require further information.

Training

Please can you describe and provide examples of how children are taught about safeguarding relating to online safety, in schools?

All schools have a statutory safeguarding responsibility (Jersey Schools Review Framework (JSRF) Appendix 5) to use a range of strategies to promote safeguarding, e.g. teaching children/young people how to stay safe, how to keep themselves from harm and how to take responsibility for their own and others' safety including when online. Schools also teach children and young people to recognise dangers and harmful situations and to know the preventive actions they can take to keep themselves safe.

Children are taught about e-safety and online harms as part of the Jersey Curriculum, for example, in Computing and PSHE in both primary and secondary. It is the intention of the Jersey Computing Curriculum that it will 'educate and empower students to use technology safely and responsibly.' The PSHE (including citizenship) content guidance provides more specific content for KS3 and KS4, e.g. [pupils should learn about] '...the opportunities and risks of forming and conducting relationships online'. Schools additionally undertake regular assemblies on these topics. Annual workshops are provided to schools on Cyber Security, including how to keep your identity safe. Schools are engaged with the Jersey Office of the Information Commissioner, who offer sessions to students on what data is and how to keep it safe.

Some schools have developed an additional Digital literacy programme to safeguard and keep children safe when using online tools, support their Digital Health and Digital Skills, and provide them with the skills needed to be effective digital citizens.

Please can you describe and provide examples of how parents / carers are informed and provided with advice by schools about children's access to online sites and online safety?

All schools have a statutory safeguarding responsibility to educate young people, parents and the school community to build knowledge, skills and capability in online safety (appendix 5 – JSRF). All schools provide advice and guidance to parents regarding online safety; links can be found on school websites.

Schools also offer workshops and parent evenings to support parents in safeguarding their children's online activities. Some schools are also testing platforms to support parents with school-managed child devices at home, including device controls and web filtering.

Please can you tell us about the online safety training that is provided to CYPES staff in schools?

All staff must complete Online Safety training as part of their regular safeguarding training. Staff also have access to the Online Safety training on Connect Learning.

Schools also run in-house training on Online Safety and Digital Skills. CYPES provide training to support effective teaching and learning in online safety to teachers where required.

Several schools hold the 360-degree online safety review tool accreditation.

CYPES has developed a Digital Strategy that includes upskilling all school staff in Online Safety and Digital Inclusion.

How much money, if any, is spent by Government of Jersey schools on specific online safety training?

There is no specific online safety training budget; however, the training we have been able to provide is funded from the CYPES central training budget. Additional funding has been provided directly by external sponsorship and by schools.

5. How do schools approach education about specific online harms or risks, for example, cyberbullying, inappropriate content, addictive behaviours, etc?

This content is re-visited regularly, and in many different contexts with the aim of developing a culture of safeguarding. For example, this content will be covered within the Jersey Curriculum for PSHE and Computing, across other subjects when opportunities arise, and through an annual cycle of assemblies and workshops. The PSHE (including citizenship) content guidance provides more specific content for KS3 and KS4, e.g. [pupils should learn about] '... how social media may distort, misrepresent, or target information in order to influence beliefs and opinions' and, within the 'Digital literacy' theme, specific content is included, such as 'how to recognise online grooming in different forms, for example in relation to sexual or economic exploitation, extremism, and radicalisation.' Teachers provide a safe and supportive learning environment and signpost students towards further support related to these issues.

To enhance the curriculum offer, schools will invite external parties to speak with students, such as the Jersey Police, Kooth and the Jersey Office of the Information Commissioner (JOIC), to speak to students on these topics. In addition to this, schools will respond to the needs and experiences of their pupils, developing specific policies to support teaching around issues, cyberbullying for example etc., in instances that occur.

Monitoring

6. How do schools fulfil their responsibilities (as per the 'Online Safety Policy') to "oversee and monitor the use of technology when children are in their care"?

(a) How is this managed consistently when the children / young people may have access to mobile phones / smart phones with internet access?

For personally owned devices used and taken into school, the web filtering policy will be applied to all devices connected to the Wi-Fi provided. Schools use their own Mobile Device Policies to manage the use of personally owned mobile devices, and parents and students must adhere to the Acceptable Usage Agreements for technology published by each school.

7. Please can you tell us about the use of Impero and other software used for the purposes of safeguarding and monitoring online access through the school IT networks?

(a) How many Government of Jersey provided schools use Impero?

All Government managed schools have Impero installed.

(b) How many Government of Jersey provided schools use another / additional software programmes? (please provide further details, for example, the software name / extent in use etc).

All Government of Jersey provided schools also have Lightspeed Filter and Lightspeed Alert. Filter and Alert provide online filtering and reporting.

(c) How many of the Government of Jersey provided schools do not have an internal monitoring system (such as Impero) to check all online activity?

None (all schools have a monitoring system)

8. Where schools have access to internal monitoring software, please could you confirm if there is specific funding provided for it from CYPES, or if the funding has to be identified and prioritised by headteachers?

Funding for these is provided by Digital Services.

9. In your opinion, should internal school technical monitoring be a legal requirement, as it is in the United Kingdom?

Under the Keeping Children Safe in Education Law 2022, schools, as corporate parents, are responsible for keeping children safe online, and technical monitoring is essential for achieving this.

10. How much money is spent by the Government of Jersey provided schools on software used for online safety purposes? Is this from the CYPES budget or the Digital Services budget?

These are funded by Digital Services.

11. The 'Online Safety Policy' states that some digital apps are able to circumvent the central monitoring and filtering systems. Please could you provide examples of where this has occurred and how frequently it is picked up by school monitoring?

No system is entirely infallible. If a Digital application is able to circumvent any filtering or monitoring, it is then actively restricted or blocked entirely to students and staff. Monitoring is ongoing and actively reported on a frequent basis. Every report is investigated and acted upon.

12. The CYPES policies highlight the importance of maintaining accurate records of online safety incidents. Please can you provide the Panel with data to confirm how many online safety incidents have been recorded across schools in the previous five years?

[If possible, please can you break down any answer to identify the types of incidents that are recorded].

Schools as Data Controllers are responsible for logging their own online safety incidents, a central record is not held.

Mobile devices

13. Is student access to harmful online content through a mobile phone (or other device) on school grounds considered as a risk by CYPES? If yes, please provide some further details about how this risk has been considered.

Lightspeed Filter protects mobile devices connected to the Wi-Fi provided in schools from harmful content. Each school also implements a Mobile Device/Acceptable Usage /BYOD policy. Through assemblies and workshops, students and staff are educated on the risks of accessing harmful online content through mobile devices.

(a) Is assessment of this risk undertaken centrally by CYPES, or at a school level?

The assessment of operational risk is undertaken at a per school level. Annual audits are undertaken by CYPES as part of a safeguarding audit to ensure the effectiveness of policies and any risk has been mitigated where possible.

The Jersey Schools Review Framework reviews safeguarding within schools, this includes online safety.

(b) If applicable, please can you describe how schools manage the risks associated with access to unfiltered and unmonitored content on mobile devices whilst on school grounds?

Schools manage the risks appropriately in accordance with their policies on a per-school basis. CYPES then reviews and audits the process to maintain consistency and effectiveness.

14. What policy options are there to reduce risk for students from accessing harmful content on mobile devices, whilst at school, in future?

Schools cover student device access and use in policies such as Acceptable Usage, Mobile Devices, BYOD and Online Safety.

15. Please can you provide the Panel with a copy of every school's mobile phone / device policy?

The Panel Officer has been provided with a copy of all policies under separate cover.

Yours sincerely,

Deputy Rob Ward
Minister for Education and Lifelong Learning

D +44 (0)1534 440152
E R.Ward2@gov.je