Government of JERSEY

Children, Young People, Education and Skills

Digital Safeguarding and Technology Use Policy

Document Purpose	Set out expectations, minimum standards and responsibilities for the safe and responsible use of digital technologies across schools, youth sites and residential care settings.
Author	CYPES Governance & Digital
Publication Date	24 November 2025
Target Audience	Teaching and support staff, site managers, governors and volunteers in education, youth services and residential care settings.
Circulation List	Teaching and support staff, site managers, governors and volunteers in education, youth services and residential care settings.
Description	The online safety policy is a safeguarding document that sets expectations and minimum standards for the safe use of digital technology across schools, youth sites and residential care settings.
Linked Policies	CYPES Acceptable Use Policy GOJ AI Policy CYPES AI Policy CYPES Data Protection Policy CYPES Data Security Policy CYPES WiFi/Unknown Network Policy CYPES Retention Schedules
Approval Route	CYPES Ministerial Team Education DLT COD DLT
Review Date	25 November 2026
Contact Details	CYPES Digital Team

Government of JERSEY

Table of Contents

1 Overview

Online safety is a core element of safeguarding. Children and young people use digital technology for learning, socialising and recreation; staff and volunteers rely on it for teaching, administration and communication. Misuse or harmful content, however, can expose children to grooming, bullying or exploitation and leave staff vulnerable to allegations.

Schools, youth sites and residential care settings have clear legal statutory duties under:

- **Data Protection (Jersey) Law 2018** which requires organisations to handle personal data fairly, lawfully and securely.
- **Children and Young People (Jersey) Law 2022** which requires organisations to promote and support the wellbeing, and safeguard the welfare, of children and young people. Schools, Colleges and Education Services must follow the guidance in Jersey's Keeping Children Safe in Education (J-KCSIE) to ensure they fulfill their duties to safeguard and promote the welfare of children and young people.
- This policy and its resources are CYPES and the Central Educations team's method to support schools, colleges and Education Services and help to mitigate any potential crimes under the **Computer Misuse (Jersey) Law 1995**.

Schools, youth sites and residential care settings must also meet the standards outlined in the Department for Children, Young People, Education and Skills (CYPES) **'Filtering and Monitoring Standards'** document to ensure appropriate systems are in place and regularly reviewed.

This policy brings those requirements together and outlines how we will protect children, staff and their data.

2 Objectives

This policy aims to:

- create a safe environment where children and young people can learn to use digital technology responsibly and build digital resilience
- set clear responsibilities for leaders, staff, parents/carers and learners to prevent and respond to online safety incidents
- define minimum technical standards – filtering, monitoring, device security and data protection
- provide processes for reporting concerns, managing incidents and referring to external agencies where necessary
- signpost further guidance.

3 Scope and responsibilities

The policy applies to all schools, youth sites and residential care settings managed or overseen by the Children, Young People, Education and Skills (CYPES) department. It covers anyone who uses digital systems on site or remotely, including learners, residents, staff, contractors, volunteers, parents/carers and community users. It applies to organisation-owned equipment and networks as well as personal devices used on premises.

To ensure the online safeguarding of children and young people, all members of our schools, youth sites, and residential care homes must work collaboratively to promote safe and responsible online behaviours. This includes learning from each other and sharing good practice, as well as reporting concerns, inappropriate behaviours or misuse as soon as these become apparent.

3.1 Senior Leadership

Headteachers in schools, or the manager of the youth site or residential care setting, hold ultimate responsibility for online safety. They must ensure that:

- robust filtering and monitoring systems are in place, regularly reviewed and aligned with statutory standards
- all staff receive appropriate training and understand their responsibilities
- digital safety is embedded across the curriculum and staff modelling
- serious incidents or allegations are managed promptly in line with safeguarding procedures
- the safety and integrity of all digital technologies including software and hardware meet minimum standards as published in the CYPES Digital and Technology Standards
- they seek assurances from third Parties including internal Digital teams that relevant minimum standards set out in the CYPES Digital and Technology standards have been met.

3.2 Governors in Schools

Governors are responsible for ensuring that the school;

- handles personal and sensitive information appropriately and lawfully
- demonstrates compliance with its duties outlined in this policy
- monitors any online safety incidents.

Governors must treat all school-related information with the highest level of confidentiality. Documents, emails, and discussions may contain sensitive information about pupils, staff, or families and must not be shared outside of the governing body or school leadership. Governors are expected to use technology responsibly and in line with this policy and the Governor's Code of Conduct.

3.3 Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL)

The DSL holds overall responsibility for all safeguarding matters. While overall responsibility for online safety cannot be delegated, the school, youth site or residential care setting may appoint an Online Safety Lead (OSL) or other relevant staff to support the DSL in delivering this function.

The DSL must:

- act as the main point of contact for online safety concerns, recording and responding to incidents appropriately
- liaise with the SLT, Governors, Police, CYPES and external agencies when necessary

- lead or coordinate annual reviews of filtering and monitoring system
- provide training, guidance and resources to staff and volunteers
- maintain awareness of emerging trends and threats, updating policies and guidance as required
- monitor the online activity of children and young people in their setting
- risk-assess and approve the use of any web-based applications that staff intend to use.

3.4 Teachers and Support Staff

All teachers and support staff must:

- demonstrate an understanding of online safety as a core part of safeguarding
- model safe, responsible and professional behaviour when using technology
- follow the Acceptable Use Policy and other relevant policies
- plan and deliver age-appropriate online safety education, promoting digital citizenship and critical thinking
- supervise learners when they use digital devices and intervene if they see misuse
- report concerns to the DSL/OSL and ensure incidents are recorded
- be aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school ensuring compliance with the 'CYPES AI Policy' as well as the 'Responsible Use of AI Guidance' for schools, youth sites and residential care homes.

3.5 IT Providers and Technicians

An IT provider can include, but is not limited to, School Technicians, Government of Jersey Digital Services and third-party providers.

IT providers and technicians (internal and external) are responsible for:

- deploying and maintaining filtering and monitoring systems that block illegal or harmful content while allowing access for teaching and learning
- ensuring systems are secure, updated and configured to minimise vulnerabilities
- supporting regular reviews and providing reports to school leaders
- liaising with the DSL/OSL when changes are required or incidents occur
- meeting the minimum standards set out in CYPES Technology Standards.

3.6 Children and Young People

Children and young people should:

- understand and follow the Acceptable Use Agreement appropriate to their age or setting
- treat others with respect when communicating online and report anything that makes them feel uncomfortable
- protect their personal information and be aware that they cannot give valid consent for processing of their data if under 13
- participate in online safety education and activities
- avoid plagiarism and uphold copyright regulations, taking care when using AI services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services

3.7 Parents and Carers

Parents and carers play a vital role in reinforcing safe behaviours. They are expected to:

- sign the Acceptable Use Agreement and support the setting in enforcing it
- supervise their children's use of technology at home and discuss online safety regularly
- report concerns to the setting and work collaboratively to resolve them.

3.8 Visitors

Visitors will:

- during school hours: access the Education Visitor Wi-Fi which requires authorisation by a staff member of the school
- outside of school hours: connect to the Government of Jersey Guest Wi-Fi. Terms and conditions are published on the Wi-Fi captive portal.

4 Policy/Standards

4.1 Acceptable Use

Acceptable Use Agreements (AUA) apply to all users. AUAs set clear expectations for behaviour when using organisation-owned or personal devices on site. CYPES templates for AUAs, for different age groups and users, can be found on the CYPES Governance, Digital and Health & Safety SharePoint site.

Key principles include:

- **Respect and courtesy:** treat others with kindness; do not send or share material that is abusive, discriminatory or likely to cause harm.
- **Content:** never deliberately access, download or share illegal or inappropriate content. Filtering systems block most harmful content, but users must act responsibly and report accidental access immediately.
- **Privacy and data protection:** do not reveal personal information about yourself or others online; comply with the Data Protection (Jersey) Law 2018 principles of lawfulness, fairness and security.
- **Security:** never share passwords. Use strong credentials and enable multi-factor authentication where available. Only install authorised software.
- **Devices and systems:** care for equipment. Do not attempt to bypass security controls or alter system settings. Respect network usage rules.
- **Digital images and social media:** obtain consent before taking or sharing photographs or videos; never post images of children or colleagues on social media without permission. Use organisation-sanctioned channels for communication with learners and parents and never use personal accounts.

Breaches of Acceptable Use Agreements will be treated seriously and may result in disciplinary action, withdrawal of access, or in severe cases, referral to external agencies.

4.2 Reporting and Responding

All online safety concerns, including inappropriate content, cyberbullying, grooming, security breaches or data loss, must be reported immediately to the DSL/Online Safety Lead. Staff and volunteers must not investigate devices and should secure devices or content, preserve evidence and inform the designated person. The DSL will assess the concern, record actions and decide whether to involve other agencies, such as CYPES, the Police, the Jersey Internet Watch Foundation or refer to Children and Families Hub.

Filtering and monitoring systems generate alerts that IT support technicians and the Online Safety Leads must check and triage alerts and act on them. Filtering and monitoring provision must be reviewed annually to assess effectiveness and to ensure policies, training and curriculum reflect emerging risks. Logs of checks must include the date, who completed the check, what was tested and any actions taken.

Incidents involving data protection, such as personal data breaches, must be reported to the setting's data protection officer without delay. Individuals have rights under the Data Protection (Jersey) Law 2018 to be informed, access, correct or delete data and to restrict or object to processing.

4.3 Use of AI (Artificial Intelligence)

AI tools offer opportunities for personalised learning and administrative efficiencies but present new risks. Staff may use AI only in accordance with the CYPES AI Policy - and the Government of Jersey's AI Policy. Key expectations are:

- Human oversight is required at all times.
- AI should be used as a tool to assist teaching and learning, not to make autonomous decisions about children or staff.
- Personal data must not be input into AI systems without a clear lawful basis and parental consent where required. Under the Data Protection (Jersey) Law 2018, children under 13 cannot consent and special category data requires additional safeguards[1].
- Staff should critically evaluate results and cross-check with reliable sources.
- Any new AI tool or system must undergo a data protection impact assessment (DPIA) and risk assessment before deployment.

4.4 Online Safety Education

Online safety education is a whole-setting responsibility. Curriculum leads must ensure that digital citizenship and safety concepts are embedded in computing, personal, social, health

[1] Data Protection (Jersey) Law 2018 "special category data" means –
(a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) genetic or biometric data that is processed for the purpose of uniquely identifying a natural person;
(c) data concerning health;
(d) data concerning a natural person's sex life or sexual orientation; or
(e) data relating to a natural person's criminal record or alleged criminal activity;

and economic (PSHE) education and across subjects. Programmes should be age-appropriate and cover topics such as (but not limited to):

- recognising and reporting abuse, grooming, exploitation and radicalisation
- respectful online behaviour and managing digital reputation
- critical evaluation of online content and misinformation
- privacy, data protection and copyright
- the benefits and risks of social media, gaming and emerging technologies
- understanding the impact of AI and algorithms
- safe use of devices at home and school.

Parents/carers should be provided with regular information and workshops to help them support safe use at home. Children and young people should be consulted through student councils or focus groups to ensure the programme reflects their experiences and needs.

4.5 Contribution of Children and Young People

Schools, youth sites and residential care settings should actively involve children and young people in shaping digital practices through structured feedback. Their insights and experiences must inform the development and evaluation of online safety strategies. This participation supports personal development, shared responsibility, and safer digital environments.

5 Technology

Schools, youth sites and residential care settings are responsible for ensuring that their infrastructure and network are as safe and secure as is reasonably practicable, and that they adhere to the CYPES Digital and Technology Standards. Where services do not meet expected standards, the school, youth site or residential care setting must liaise with CYPES Governance and Digital to address any technical or data protection concerns.

5.1 Devices and Security

All organisation-owned devices must:

- be registered and configured centrally with approved operating systems, firmware and anti-malware software
- use encryption and secure passwords
- have remote-wipe capabilities where feasible.

Personal devices may only connect to networks where bring-your-own-device (BYOD) arrangements are approved. The network should restrict access to sensitive resources, and monitoring must still apply.

5.2 Filtering and Monitoring

Schools, youth sites and residential care settings must have in place technical controls to block illegal, harmful, or inappropriate content without unreasonably impacting teaching and learning.

Filtering is a preventative tool that blocks access to unsafe content using blocklists (e.g. Internet Watch Foundation) and must be tailored to different user groups (e.g. staff vs

learners). It should be regularly reviewed based on user risk profiles, technical limitations, and curriculum needs, with logs retained for inspection.

Monitoring tracks user activity to identify safeguarding risks. It helps detect misuse, supports timely intervention, and ensures accountability. While filtering prevents access, monitoring provides visibility into behaviour and supports safeguarding responses.

Online harm refers to the risks and negative impacts that children and young people may encounter when using digital technologies and the internet. These harms are typically grouped into four key categories:

1. **Content** – Exposure to illegal, inappropriate, or harmful material.
   Examples: pornography, self-harm content, hate speech, misinformation, radicalisation.
2. **Contact** – Harmful interactions with others online.
   Examples: grooming, cyberbullying, coercion, peer pressure, impersonation.
3. **Conduct** – Personal online behaviour that increases the risk of harm.
   Examples: sharing explicit images, engaging in abusive or disrespectful communication, oversharing personal information.
4. **Commerce** – Risks related to financial exploitation or scams.
   Examples: phishing, online gambling, fraudulent advertising, in-app purchases targeting children.

An **'online safety incident'** is any occurrence in a school, youth site or residential care setting where the use of digital technology results in actual or potential harm to individuals, violates safeguarding policies, or breaches the acceptable use policy outlined above.

Examples of online safety incidents include, but are not limited to:

- cyberbullying between children and young people or involving staff
- accessing or sharing inappropriate or illegal content
- online grooming or exploitation
- hacking or unauthorised access to school systems
- sharing personal data without consent
- use of technology for extremist or radicalising content

All sites must log all online safety incidents without delay, following updated central processes.

5.3 Data Protection

Under the Data Protection (Jersey) Law 2018, personal data must be used lawfully, fairly and transparently, kept accurate, used only for specified purposes, stored no longer than necessary and protected with appropriate security. Sensitive data (such as health or ethnicity) requires additional safeguards. Children under 13 cannot consent to data processing; parents/carers must provide consent. Staff should complete data protection training and follow the organisation's privacy notices and retention schedules.

Each data controller must appoint a qualified, impartial Data Protection Officer (DPO) and maintain a Data Protection Inventory detailing what personal data is held, where, why, and who is responsible for it.

5.4 Cyber Security

Cyber Security is an essential component in safeguarding and referred to in Jersey KCSIE.

Schools, youth sites and residential care settings must follow a recognised cyber security framework (for example, Cyber Essentials) that must include:

- regular risk assessments and penetration testing
- controlling and reviewing user privileges
- maintaining offline or cloud backups and testing restoration procedures
- patching and updating systems promptly
- reporting cyber incidents to the relevant authority and the Jersey Office of the Information Commissioner (JOIC) where required
- all users with access to managed systems must receive training on the common cyber security threats and incidents e.g. phishing attacks, this includes all staff and governors.
- have a business continuity and incident management plan in place

6 Further information and related documents

CYPES Acceptable Use Policy
GOJ AI Policy
CYPES AI Policy
CYPES Data Protection Policy
CYPES Data Security Policy
CYPES Retention Schedules
Digital Harms Guidance – Staff
Digital Harms Guidance – Children and Families
Jersey Keeping Children safe Online Guidance
CYPES Wi-Fi/Unknown Networks Policy

All operational guidance and internal processes for schools, youth sites and residential care settings related to this policy can be found in the CYPES Governance, Digital and Health and Safety internal SharePoint site.

7 Glossary

Term	Definition
Acceptable Use Agreement (AUA)	A formal agreement outlining expectations and rules for responsible and appropriate use of digital technology and systems. May vary by role (e.g. learner, staff, parent/carer).
CYPES	Children, Young People, Education and Skills – Government of Jersey department responsible for education, safeguarding and digital policy within the sector.
Digital Resilience	A child or young person's ability to recognise, manage, and recover from online risks and challenges, promoting healthy digital habits.
Designated Safeguarding Lead (DSL)	A trained staff member with lead responsibility for safeguarding, including online safety, within a school, youth site, or care home.
Flagged Terms	Keywords or phrases that trigger alerts or filtering in monitoring systems due to their association with harmful or inappropriate content.
Filtering	The technology used to restrict or block access to certain online content based on predetermined categories or flagged terms.
Monitoring	Systems or processes used to review and track users' digital activity to identify safeguarding risks or policy breaches.
Managed Device	A digital device that is owned and configured by the school, youth site, or residential care home and subject to safeguarding and technical controls.
Online Safety Incident	Any occurrence in a school, youth site or residential care setting where the use of digital technology results in actual or potential harm to individuals, violates safeguarding policies, or breaches the acceptable use policy.
Online Safety Lead (OSL)	A role that supports the DSL by overseeing online safety education, curriculum, incident logging and staff training.
Parental Controls	Digital settings applied to devices or platforms to restrict access to content or functions, particularly for safeguarding children and young people.
Safeguarding	The proactive approach to promoting the welfare of children and protecting them from harm, including in online environments.
Youth Site	A non-educational setting where youth engagement activities take place, typically operated under the CYPES framework.
Residential Care Home	A regulated living setting for children and young people who are in care, where staff are responsible for their daily welfare and safeguarding, including online safety.
Digital Harms	Risks and negative experiences encountered through the use of digital technology, such as cyberbullying, exploitation, or exposure to harmful content.
Artificial Intelligence (AI)	Software or systems that simulate human intelligence for tasks such as content generation, risk detection, or decision support. Use of AI must be transparent, ethical, and human-supervised.

Term	Definition
Device Management	Procedures and controls for configuring, monitoring and maintaining devices (particularly personal or unmanaged ones) to ensure online safety and compliance.
Web-based Application	Any software or service accessed through a web browser, which may require safeguarding review before use in educational or care settings.

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change
1	24/11/2025	CYPES	First Publication
			Review
			Update

APPROVAL

Presented To	Approval Date
CYPES Ministerial Team	20/11/2025