

Acceptable Use of Technology & Online Safety Policy

Document number	2-11
Applies to	All Educ8 schools and provisions
Issue	3-0
Author	Director – Finance, HR, People and Development
Portfolio Director	Director of Education, Safeguarding & Standards
Approved by	Executive Board
Effective date	1 September 2026
Next review due by	1 September 2027

2. Issue and Revision History

Issue	Description	Author	Effective date
1.0	Initial release	J. Payne	01/09/2013
2.0-2.7	Annual reviews and updates, including Google Workspace and changes to KCSIE	Various	2014-2021
2.8	Substantial rewrite aligned to KCSIE 2022	T. Warner	01/09/2022
2.9	Filtering and monitoring updates aligned to KCSIE 2023	T. Warner	01/09/2023
2.10	Updates aligned to KCSIE 2024	T. Warner	26/04/2024
2.11	Annual review aligned to KCSIE 2025; expanded risk assessment, Google Workspace, AI and filtering and monitoring content	T. Warner	26/08/2025
3.0	Full rewrite, including title change, aligned to KCSIE 2026, current Independent School Standards, DfE digital standards, statutory mobile phone guidance and revised RSHE guidance. Added responsibilities, AI requirements, incident routes, staff agreement and auditable filtering and monitoring review schedule.	T. Warner	01/09/2026

3. Summary

Online safety is an integral and interrelated part of Educ8's whole-school safeguarding arrangements. This policy sets out how Educ8 protects and educates learners, staff and other users in their use of technology and how it identifies, intervenes in and escalates online safety concerns.

The policy applies to Educ8-provided and personally owned technology used for an Educ8-related purpose. It covers acceptable use, mobile and smart technology, generative artificial intelligence, online safety education, information security, data protection, filtering and monitoring, remote education, social media and the response to incidents or concerns.

No technical system can eliminate all online risk. Educ8 therefore combines proportionate technical controls with effective supervision, education, professional curiosity, clear reporting routes and timely safeguarding action.

Failure to comply with this policy may result in withdrawal of access, action under relevant behaviour, disciplinary or contractual procedures, safeguarding action and, where appropriate, referral to external agencies or the police.

4. Document Release

This document has been reviewed in accordance with the Educ8 Quality System, current statutory guidance and the requirements applicable to Educ8's schools and provisions.

Following approval, relevant staff will be informed of its publication and any material changes to its content. Appropriate guidance or training will be provided where required to support effective implementation.

Where the policy is published electronically, the previous version will be removed or archived and replaced by the approved version. The effective date shown on the document indicates the date from which this version applies.

This policy will be reviewed at least annually and sooner where required by changes to legislation or statutory guidance, developments in technology, identified safeguarding risks, significant incidents or concerns about the effectiveness of Educ8's arrangements.

The policy will be reviewed by the Director with portfolio responsibility for Education, Safeguarding and Standards before being presented to the Executive Board for final approval.

5. Purpose

Educ8 is committed to safeguarding and promoting the welfare of every child and young person in its care. This policy establishes clear expectations for the safe, responsible, respectful and lawful use of technology by learners, staff and other members of the Educ8 community.

Online safety is an integral and interrelated part of Educ8's whole-school approach to safeguarding. This policy supports compliance with Keeping Children Safe in Education 2026, the Education (Independent School Standards) Regulations 2014 and other relevant legislation and statutory guidance.

The purpose of this policy is to:

- protect learners and staff from illegal, inappropriate or harmful online content, contact, conduct and commercial activity;
- educate learners to use technology safely, critically, respectfully and responsibly;
- establish clear requirements for the acceptable use of Educ8's devices, accounts, networks, systems and information;
- ensure appropriate arrangements are in place for filtering, monitoring and responding to online safety concerns;
- support the safe and responsible use of personal devices, mobile technology, digital services and generative artificial intelligence;
- protect personal, confidential and safeguarding information; and
- ensure online safety, cyber-security, technical and data-protection concerns are reported promptly and managed appropriately.

Educ8 recognises that technology and associated risks develop rapidly. Its arrangements will therefore be reviewed regularly and informed by statutory guidance, emerging risks, incident information, the needs and vulnerabilities of learners and the views of learners, staff and parents or carers.

6. Scope

This policy applies across all Educ8 schools, alternative provision settings and other education services. It applies to:

- members of the Executive Board and anyone undertaking governance responsibilities;
- Executive Heads, Headteachers and other senior leaders;
- all employees, including teaching, support, administrative and central staff;
- agency and supply staff, contractors, consultants, trainees, apprentices and volunteers;
- learners;
- parents and carers when accessing Educ8 systems or digital services; and
- visitors and any other person given access to Educ8's devices, networks, accounts, systems or information.

The policy applies on Educ8 premises, during educational visits and work experience, while providing or receiving remote education, when working remotely and whenever technology is used for an Educ8-related purpose.

It applies to both Educ8-provided and personally owned technology, including computers, Chromebooks, laptops, tablets, mobile phones, smart watches, cameras, recording devices, removable storage, networks, Wi-Fi, personal hotspots, email, Google Workspace, social media, messaging services, learning platforms, video-conferencing, applications, generative artificial intelligence and other current or emerging technologies.

The requirements apply whenever a person uses an Educ8 device, account, network or digital service; uses a personal device or account for an Educ8-related purpose; creates, accesses, stores, records or shares Educ8 information; communicates on Educ8's behalf; or engages in online conduct outside Educ8 which may affect the safety or welfare of a learner, another member of the Educ8 community, the orderly operation of a school or Educ8's reputation.

All users must comply with this policy, the relevant Acceptable Use Agreement and associated procedures.

7. Legal and Regulatory Framework

This policy has been prepared with regard to the following legislation, standards and guidance, as amended or replaced from time to time:

Keeping Children Safe in Education 2026;
Working Together to Safeguard Children 2026;
the Education (Independent School Standards) Regulations 2014, particularly Parts 1, 3 and 8;
the Prevent Duty guidance and related safeguarding risk assessment requirements;
the DfE Filtering and Monitoring Core Standard and Cyber Security Core Standard;
DfE statutory guidance on Mobile Phones in Schools;
the statutory Relationships Education, Relationships and Sex Education and Health Education guidance for introduction from September 2026;
DfE guidance on Generative Artificial Intelligence in Education and Generative AI Product Safety Standards;
the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025;
the Equality Act 2010;
the Computer Misuse Act 1990;
the Copyright, Designs and Patents Act 1988; and
the Online Safety Act 2023, where relevant to services used by Educ8 and the online environment experienced by learners.

Status of guidance: KCSIE 2026 and the revised RSHE and mobile phone expectations apply from 1 September 2026. Educ8 will consider and document any justified departure from statutory guidance which states that schools should or should not take a particular action.

8. Definitions and Acronyms

Term	Definition
AUP	Acceptable Use Policy or Agreement setting out the conditions under which technology may be used.
BYOD	Bring Your Own Device: an expressly authorised arrangement under which a personally owned device is used for an Educ8 purpose.
DSL	Designated Safeguarding Lead. The DSL retains lead responsibility for safeguarding and online safety and may be supported by trained deputies.
DPO	Data Protection Officer.
Filtering	Preventative technical controls intended to block access to illegal, inappropriate or potentially harmful online content.
Generative AI	Technology capable of generating or altering text, images, audio, video, code or other material in response to user input.
IT support	Internal or contracted technical support responsible for maintaining systems and implementing authorised technical changes.
KCSIE	Keeping Children Safe in Education, the current statutory safeguarding guidance for schools and colleges.
Monitoring	Technical or in-person arrangements used to observe, review or record activity so that concerns can be identified and acted upon.
Online safety	Safeguarding learners and other users from risks arising from technology and supporting safe, responsible and informed use.

Term	Definition
Learner	Any child receiving education or support from Educ8.
Filtering and monitoring lead	The Headteacher of each school, acting as the assigned member of senior leadership responsible for ensuring that filtering and monitoring arrangements are implemented effectively within their school.
User	Any person using an Educ8 device, account, system, service, network or information.

9. Roles and Responsibilities

Online safety is a shared responsibility. Responsibilities are allocated as follows:

Role	Principal responsibilities
Individual proprietor(s)	The individual proprietor or joint proprietors of each registered independent school retain legal responsibility for ensuring that the school meets the Independent School Standards and its statutory safeguarding duties. This includes ensuring that appropriate online safety, filtering and monitoring arrangements are established, adequately resourced, reviewed and operating effectively.
Executive Board	Provides strategic governance, scrutiny and assurance across Educ8 in accordance with the Governance & Leadership Handbook. It approves this policy; considers significant online safety, filtering and monitoring, cyber-security and data protection risks; and holds executive and school leaders to account for addressing identified weaknesses. The Executive Board's governance arrangements do not remove or transfer the legal responsibilities of the individual proprietor or joint proprietors of each school.
Portfolio Director – Education, Safeguarding & Standards	Acts as the responsible governance representative for filtering and monitoring. Provides scrutiny, challenge and assurance; is involved in the annual filtering and monitoring review; considers identified risks, control failures and improvement actions; and reports assurance or concerns to the Executive Board. The Portfolio Director does not undertake operational management of filtering and monitoring arrangements.
Executive Heads	Provide strategic leadership, support and challenge to Headteachers. Promote consistency across Educ8; ensure that significant or recurring concerns are escalated; monitor completion of agreed improvement actions; and ensure that online safety is considered through school improvement, safeguarding, curriculum, behaviour, SEND and staff-development arrangements.
Head of Safeguarding & Awarding Organisation Compliance (Group DSL)	Provides strategic safeguarding leadership, coordination and professional assurance across Educ8. Reviews relevant reports, incidents, trends and emerging risks; promotes consistency between schools; coordinates the Educ8-wide evaluation of filtering and monitoring effectiveness; supports DSLs and DDSLs; and advises the Executive Leadership Team and Executive Board on safeguarding risks and required improvements. This role does not replace the operational accountability of each Headteacher.
Headteachers	Each Headteacher is the assigned senior leadership lead responsible for ensuring that filtering and monitoring arrangements are implemented effectively within their school. Headteachers ensure that local risks are assessed; staff understand their responsibilities; learners are appropriately supervised; filtering and monitoring reports are acted upon; requests to block or allow access are appropriately considered and recorded; failures are reported and escalated; and agreed actions are

Role	Principal responsibilities
	completed. Headteachers participate in the annual review of filtering and monitoring provision.
School DSLs and DDSLs	Lead the safeguarding response to online safety concerns within their school. Receive and review relevant alerts and monitoring information; assess risk to individual learners and others; ensure that concerns and decisions are recorded on CPOMS; make or coordinate referrals where required; support affected learners; identify patterns and emerging risks; and contribute to risk assessments and the annual filtering and monitoring review.
IT support	Provides technical expertise and implements, maintains and tests Educ8's approved filtering, monitoring, cyber-security and access controls. IT support manages authorised technical changes; maintains appropriate system and audit logs; investigates and reports technical failures; preserves relevant technical evidence; supports the annual review; and promptly escalates safeguarding concerns, significant system failures and cyber incidents through the appropriate routes. Reporting to IT support does not replace reporting to the DSL or DDSL where there is a safeguarding concern.
Data Protection Officer (DPO)	Advises on compliance with data protection law and Educ8's data protection policies. Provides advice on the lawful and proportionate use of monitoring information; supports the assessment and management of personal data breaches; and advises on data protection impact assessments where new technology or monitoring arrangements create a potentially high risk to individuals' rights and freedoms.
All staff, agency workers, contractors and volunteers	Must comply with this policy, the Staff Acceptable Use Agreement, the Staff Behaviour Policy and safeguarding procedures. They must use Educ8 technology responsibly; maintain appropriate professional boundaries; supervise learners appropriately; complete required training; protect accounts and information; and report safeguarding concerns, filtering failures, cyber incidents, data breaches and inappropriate use immediately through the specified routes.
Learners	Must use technology in accordance with the Learner Acceptable Use Agreement and instructions given by staff. Learners should behave safely and respectfully online; protect passwords and personal information; avoid attempts to bypass technical controls; and report harmful content, inappropriate contact, security concerns or accidental access to unsuitable material to a trusted adult.
Parents and carers	Are encouraged to support Educ8's online safety expectations; discuss safe and responsible technology use with their child; raise relevant concerns promptly; and work with the school where support, education or safeguarding action is required.

Educ8 role allocation: Each Headteacher is the assigned senior leadership lead responsible for ensuring that filtering and monitoring arrangements are implemented effectively within their school. The Head of Safeguarding & Awarding Organisation Compliance, who is the Group DSL, provides group safeguarding leadership, coordination, review and professional assurance. School DSLs and DDSLs lead safeguarding responses within their schools. IT support provides technical expertise, maintains and tests the approved technical controls and reports identified concerns or failures through the appropriate safeguarding and operational routes. The Education Portfolio Director provides governance scrutiny, challenge and assurance, while the Executive Board provides overall strategic governance.

10. Online Safety and Acceptable Use

10.1 The four areas of online risk

Educ8 uses the four areas of risk described in KCSIE as the basis of its online safety arrangements:

Risk	Examples
Content	Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.
Contact	Harmful interaction with other users or generative AI applications which simulate interaction, including peer pressure, grooming, exploitation, coercion, commercial advertising and adults posing as children or young adults.
Conduct	Online behaviour which causes or increases the likelihood of harm, including bullying, harassment, abuse, impersonation and making, sending or receiving explicit images, including images created or altered using AI.
Commerce	Risks including gambling, inappropriate advertising, phishing, scams, financial exploitation, in-app purchasing and financially motivated sexual extortion.

Risks may overlap and may occur on school systems, personal devices, social media, gaming platforms, messaging services or emerging technologies. Concerns are not dismissed because the activity occurred away from Educ8 premises or outside school hours.

10.2 Online safety risk assessment

Educ8 will complete a documented online safety risk assessment at least once every academic year and review it following significant incidents, material technology changes or identified concerns. Each site will ensure that group controls are supplemented by local information where risks differ.

The assessment will consider:

the age, needs and vulnerabilities of learners, including SEND, EAL, looked-after children, children with social workers and learners at risk of exploitation or radicalisation;
the Prevent risk assessment and relevant local safeguarding influences;
learner and staff use of devices, networks, personal hotspots, BYOD, remote access and off-site learning;
filtering and monitoring coverage, limitations, checks, alerts and incident information;
the use or potential unauthorised use of generative AI and dynamic or personalised content;
curriculum and teaching requirements, including the need to avoid unreasonable over-blocking;
learner voice, including learners' wishes, feelings and lived experiences where relevant; staff feedback; parent and carer concerns; and national or local trends; and
identified actions, owners, deadlines and evidence of completion.

10.3 General acceptable use requirements

All users must:

use Educ8 technology and information only for authorised, lawful and appropriate purposes;
use their own account, keep credentials secure, use strong unique passwords and multi-factor authentication where provided, and lock or sign out of devices when unattended;
respect other people, their privacy, intellectual property and work;
not attempt to bypass filtering, monitoring, access controls or other security measures, including by using VPNs, proxy services, translation tools, personal hotspots or unauthorised accounts;
not access, create, store or share illegal, abusive, discriminatory, threatening, sexually explicit or otherwise harmful material;
not install software, extensions or applications or connect removable media without authorisation;

not access another person's account, files or communications without authority;
protect personal, confidential and safeguarding information and use only approved storage and communication services;
report accidental access, suspicious activity, harmful content, technical failures, lost devices or security concerns promptly; and
understand that authorised and proportionate monitoring may take place in accordance with this policy and Educ8's privacy information.

Reporting accidental access or a genuine concern will not, by itself, result in a sanction. Deliberate concealment, repeated misuse or attempts to bypass controls may result in action.

10.4 Mobile phones and smart technology

Educ8 schools will be mobile phone-free environments by default. Learners will not have access to mobile phones, smart watches or personal communication or recording devices throughout the school day, including lessons, movement between lessons, breaks and lunchtime.

Devices brought to school must be switched off and handed in or stored securely in accordance with the site's published arrangements.

Any exception must be authorised by the Headteacher, documented and based on an identified medical, SEND, safeguarding or other exceptional need.

An authorised exception does not permit unrestricted use and must specify when, where and how the device may be accessed.

Learners must not use personal hotspots or personal devices to bypass school controls.

Personal devices must not be used to photograph, film or record another person without authority and appropriate consent.

Staff personal devices must be kept out of use while supervising or teaching learners except for an authorised operational or emergency purpose. Images, recordings or learner information must not be stored on personal devices.

Local arrangements, reasonable adjustments, searching and confiscation and any sanctions will be consistent with Educ8's Behaviour Policy, statutory guidance and the individual circumstances of the learner.

10.5 Generative artificial intelligence and emerging technology

No new digital service, AI tool, browser extension or learner-facing application may be introduced without appropriate approval. The assessment must consider intended use, age restrictions, safeguarding, filtering and monitoring, privacy, data processing, intellectual property, equality, accessibility, educational benefit, cyber security and contractual terms.

Users must:

- use only tools approved for the relevant purpose and user group;
- never enter identifiable learner, staff, safeguarding, medical, financial, confidential or special-category information into an unauthorised AI service;
- comply with the age restrictions and terms of the tool;
- critically review AI outputs for accuracy, bias, safety, appropriateness and copyright concerns;
- remain professionally responsible for any final content, decision, communication or resource;
- not use AI to impersonate others, create misleading communications, generate abusive or sexualised material, facilitate cheating or circumvent assessment rules; and
- clearly acknowledge AI assistance where required by Educ8 or an awarding organisation.

Learner-facing use must have clear educational benefit, appropriate supervision and suitable product-level safety, filtering and monitoring features. Educ8 will not rely solely on an AI provider's safeguards. AI will not make final safeguarding, disciplinary, admissions, employment or other significant decisions about individuals.

10.6 Teaching online safety

Online safety will be a planned and progressive part of the curriculum, including PSHE, RSHE, computing and wider learning. Teaching will be age-appropriate, responsive to identified risks and designed to develop knowledge and behaviour that transfer across devices, platforms and applications.

Learners will be taught, as appropriate, about:

the four areas of risk and how risks overlap;
privacy, personal information, passwords, consent and online reputation;
respectful relationships and the fact that the same standards of behaviour apply online and offline;
grooming, exploitation, coercion, sexual harassment, sharing nudes and semi-nudes and financially motivated sexual extortion;
cyberbullying, discriminatory abuse, misogyny, racism, homophobia and harmful language presented as banter;
misinformation, disinformation, conspiracy theories, persuasive design, advertising, scams and gambling;
AI-generated content, deepfakes, deep nudes, bias, hallucinations and responsible AI use;
copyright, ownership, academic integrity and the responsible creation and sharing of content;
how filtering and monitoring work, their purpose and limitations; and
how to report concerns, block or report users and access trusted help.

Teaching will not rely on fear or lists of prohibited actions. It will help learners assess situations, understand consequences, make informed decisions, disengage from harmful contact and seek help.

10.7 Additional vulnerability and accessibility

Any learner can be vulnerable online. Educ8 recognises that learners with SEND, communication needs, trauma, social care involvement or other vulnerabilities may face additional barriers to recognising risk, reporting concerns or recovering from online harm.

Teaching, supervision, filtering profiles, reporting methods and support will therefore be adapted where necessary. Reasonable adjustments will not reduce safeguarding expectations but will enable learners to understand and comply with them.

10.8 Whole-school approach and training

Online safety will be reflected across safeguarding, behaviour, anti-bullying, curriculum, staff behaviour, mobile phone, data protection, remote education and relevant operational procedures.

All staff will receive safeguarding and child protection training, including online safety and their filtering and monitoring responsibilities, at induction.

Training will be regularly updated and staff will receive online safety updates as required and at least annually. Relevant leaders, the DSL and IT support will receive role-specific and system-specific training.

The Executive Board and responsible Director will receive sufficient information and training to provide effective challenge and assurance.

Staff and learner feedback will inform arrangements and policy review.

10.9 Remote education

The same safeguarding, professional conduct, acceptable use, data protection and reporting expectations apply during remote education and online communication as when learners are physically present.

Only Educ8-approved accounts and platforms may be used for live teaching or direct communication with learners.

Staff must use appropriate professional environments, language and boundaries and follow safer working practice guidance.

Learners and parents must be told what platform will be used, who the learner will interact with, what will be recorded, and how to report a concern.

One-to-one remote contact must be specifically authorised and managed in accordance with safeguarding and safer working arrangements.

Recordings may only be made where authorised, necessary, transparent and compliant with data-protection requirements.

Any concern arising during remote education must be reported through the usual safeguarding route without delay.

11. Managing Information Systems

11.1 Information security and access management

Educ8 will take proportionate measures to protect learners, personal information and service continuity. Its arrangements will be informed by the DfE Cyber Security Core Standard and its wider safeguarding responsibilities.

Each user will have an individual account with access limited to what is required for their role or education. Multi-factor authentication will be applied where required by Educ8's security arrangements.

Accounts and permissions will be created, changed, reviewed and removed promptly, including when a person leaves or changes role.

Devices and software will be supported, patched and updated; unsupported systems will not be used for sensitive or learner-facing activity.

Malware protection, secure configuration, backups, recovery arrangements and asset registers will be maintained as appropriate.

Personal data will only be accessed, transferred and stored using authorised devices and services.

A cyber risk assessment will be completed annually and reviewed at least termly, with a documented incident-response and recovery plan.

11.2 Google Workspace for Education

Google Workspace for Education is Educ8's principal cloud collaboration and communication environment. Google Workspace controls are one component of Educ8's safeguarding and security arrangements and are not treated as a complete filtering or monitoring solution on their own.

Learner and staff accounts will be placed in appropriate organisational units with permissions and services configured for the relevant user group.

Sharing, external communication, application access, account recovery and administrative privileges will be restricted according to need and risk.

Learner-use Chromebooks must be formally enrolled and managed before issue.

Guest logins and personal account use on learner devices will be blocked where technically possible and consistent with the approved configuration.

Audit and security logs will be made available to authorised staff and used in accordance with this policy and retention arrangements.

Changes to Google Workspace configuration will be authorised, tested and recorded.

11.3 Filtering

Educ8 will maintain active and well-managed filtering designed to prevent access to illegal, inappropriate and potentially harmful content without unreasonably restricting teaching, safeguarding education or administration.

Filtering will apply to all school-managed devices, including those taken off-site, and to all Educ8 sites and relevant networks.

Approved arrangements will address guest users, unmanaged devices and any expressly authorised BYOD use, including use of separate networks where appropriate.

At a minimum, learner and staff profiles will provide appropriately different levels of access.

The filtering solution will implement current IWF and CTIRU blocklists and prevent users from disabling, overriding or altering those protections.

Controls will address common circumvention methods, including VPNs, proxies, anonymisers and personal hotspots, so far as reasonably practicable.

Local additions, exceptions and over-blocking decisions will be authorised, documented and reviewed.

Filtering for real-time, dynamic, personalised and AI-generated content will be considered within the risk assessment and procurement process.

No filtering system is completely effective. Accidental access or an apparent gap must be reported immediately so that safeguarding and technical action can be considered.

11.4 Monitoring

A formal review of filtering and monitoring provision will be completed at least once in each academic year and following any significant incident, material system change or identified control failure. The review will be coordinated by the Head of Safeguarding & Awarding Organisation Compliance and undertaken with each Headteacher, as the assigned senior leadership lead, relevant school DSLs or DDSLs and IT support. The Education Portfolio Director will be involved through governance scrutiny and challenge and will provide assurance to the Executive Board. Findings, risks, actions, owners and completion dates will be formally recorded.

Staff supervising learners using devices will conduct active in-person monitoring and remain alert to the use of other devices or workarounds.

The monitoring plan will identify how school-managed devices are monitored on-site and off-site.

Monitoring reports highlighting incidents will be provided and reviewed at least weekly.

High-risk safeguarding, malicious or technical activity will be reported immediately to the appropriate responsible person.

Reports and alerts will be understandable, attributable to an identifiable user where reasonably possible and reviewed by authorised staff.

The DSL will decide and lead safeguarding action arising from monitoring information.

Incidents, decisions, actions and outcomes will be recorded so that trends and effectiveness can be evaluated.

Users will be informed that filtering and monitoring take place through this policy, AUPs, privacy information and appropriate device or login notices.

Monitoring will be lawful, fair, transparent and proportionate. Where a technical monitoring solution processes personal information, Educ8 will complete or review a DPIA, privacy information, contractual safeguards and retention arrangements before use.

11.5 Review and testing of filtering and monitoring

A formal review of the effectiveness of filtering and monitoring will be completed at least once every academic year. It will be led by the SLT filtering and monitoring lead with the support of the DSL and IT support and will involve the responsible Director.

The review and associated checks will:

cover all internet-connected devices, user groups, networks, sites and relevant locations;

include devices used off-site and assess any guest, unmanaged-device, BYOD, hotspot and remote-access arrangements;

confirm that filtering is functioning, profiles are appropriate and required blocklists are applied;

test monitoring reports, alert routes, response times and recording arrangements;

consider learner risk, SEND, EAL, incidents, Prevent, curriculum needs and AI use;

identify limitations, gaps, over-blocking and required procurement or configuration changes;

record what was checked, when, by whom, the results, actions, owners and deadlines; and

be made available to the Executive Board, inspectors and other authorised persons.

Additional checks will be completed at least termly and following material system or equipment changes, a significant incident, a reported failure or a change in identified risk. New devices and services must be checked before release to users.

11.6 Email, messaging and communications

Staff must use Educ8-approved accounts and platforms for professional communication and communication with learners.

Personal email, social media or messaging accounts must not be used to communicate with learners or store or transmit Educ8 information.

Learners may use only accounts and communication services authorised for them and must report offensive, suspicious or unsafe communications.

Communications must be professional, respectful, necessary and appropriate and must not disclose personal or confidential information without authority.

Users must remain alert to phishing, impersonation, malicious links, payment diversion and AI-generated scams and report suspicious messages promptly.

Group, wellbeing or reporting inboxes must have a named owner, appropriate access, regular monitoring and suitable cover arrangements.

Forwarding chain messages, spam or harmful content is prohibited.

11.7 Published content, learner work and images

Websites, social media and other public content must be authorised, accurate, accessible, respectful and consistent with safeguarding, privacy, copyright and Educ8's communications arrangements.

Personal contact information for learners or individual staff will not be published unless specifically authorised and necessary.

Images and recordings will be selected carefully so that they do not expose learners to avoidable risk, disclose sensitive information or enable inappropriate reuse.

The appropriate lawful basis and, where required, valid consent will be established before learner images, recordings or identifiable work are published.

Consent and safeguarding suitability are separate considerations; content will not be published merely because consent exists.

Names, location data, uniforms, routines and other contextual information will be considered together when assessing identification risk.

AI-generated or altered content must be checked and must not misleadingly represent a real learner, member of staff or event.

Requests to remove content will be considered promptly in accordance with safeguarding and data-protection requirements.

11.8 Official and personal social media

Only authorised personnel may establish or administer an Educ8 social-media account.

Administrative access must be retained by Educ8, protected by appropriate security and capable of transfer when staff change.

Official accounts will be moderated and used only for approved purposes.

Staff must not accept or initiate personal social-media connections with current learners and must maintain appropriate professional boundaries with former learners.

Staff must not discuss confidential Educ8 matters, identify learners or post content which undermines safeguarding, professional standards or Educ8's reputation.

Online concerns affecting learners or the school community must be reported even where they arise on personal accounts or away from Educ8 premises.

11.9 Personal data and privacy

Personal data will be processed in accordance with applicable data-protection legislation and Educ8's policies, privacy notices and retention schedule.

Only the minimum necessary information will be accessed, used or shared for an authorised purpose.

Personal data must not be stored in personal accounts, consumer messaging applications, unauthorised cloud services or personal devices.

Sensitive information sent electronically must use approved secure methods and appropriate access controls.

Personal or confidential information must not be entered into an unauthorised generative AI tool.

Users must promptly report misdirected communications, lost devices, unauthorised access, accidental disclosure or other suspected data breaches.

Monitoring data and logs will be accessible only to authorised staff and retained for no longer than required by the approved retention arrangements.

11.10 Administrative access, logs and audit

Administrative access will be restricted to authorised individuals, protected by strong authentication and used only for legitimate operational, safeguarding, security or legal purposes. Privileged actions will be logged where the system permits and administrative access reviewed regularly.

Logs, messages and files may be preserved and reviewed where necessary and proportionate to investigate a safeguarding concern, security incident, suspected misuse, legal obligation or complaint. Staff must not conduct informal searches or investigations without authority.

12. Responding to Concerns, Incidents and Complaints

12.1 Reporting routes

Concern	Immediate route
Learner safeguarding or harmful online activity	Report immediately to the DSL or DDSL and record the concern on CPOMS in accordance with Educ8's Safeguarding & Child Protection Policy. Recording a concern on CPOMS does not replace direct notification to the DSL or DDSL where immediate action may be required.
Filtering failure or unsuitable material accessible	Report to IT support and the Headteacher. Where a learner or safeguarding risk is involved, also report immediately to the DSL or DDSL.
Cyber incident, suspicious account activity or malware	Report immediately to IT support and the Headteacher and follow the Cyber Incident Response Plan. Escalate to the relevant Executive Head, DPO, Head of Safeguarding or Executive Board as required by the nature and seriousness of the incident.
Actual or suspected personal-data breach	DPO and IT support immediately; preserve relevant evidence.
Concern or allegation about an adult	Report immediately to the Headteacher in accordance with Educ8's Safeguarding & Child Protection Policy and Staff Behaviour Policy. Where the concern relates to the Headteacher, report it without first notifying the Headteacher to the registered proprietor for a registered independent school, or a director of the company operating an alternative provision setting, whose role must be expressly identified in the Safeguarding & Child Protection Policy. Where the concern relates to the proprietor, follow the direct LADO/local authority reporting route set out in that policy.
Low-level concern about an adult	Report promptly to the Headteacher in accordance with Educ8's Low-Level Concerns Procedure. A low-level concern about the Headteacher must be reported to the registered proprietor for a registered independent school, or a director of the company operating an alternative provision setting. Reporting to IT support does not replace reporting to the DSL or DDSL where there is a safeguarding concern.
Concern about safeguarding practice	Use the Whistleblowing Policy where normal reporting is unavailable, inappropriate or has not addressed the concern.
General dissatisfaction	Complaints Procedure, after any immediate safeguarding, technical or data-protection actions have been taken.

Where a concern falls into more than one category, all relevant leads must be informed. Reporting to IT support does not replace reporting to the DSL where there is a safeguarding concern.

12.2 Safeguarding response

The DSL will consider the immediate safety of the child; their wishes, feelings and lived experiences; the risk to others; preservation of evidence; parental communication; internal support; and whether referral to children's social care, the police, CEOP, Prevent/Channel or another agency is required.

Online child-on-child abuse will be taken as seriously as abuse occurring face to face. Educ8 will respond where online behaviour occurs off-site if it raises safeguarding concerns, affects learners' welfare, disrupts education or involves members of the Educ8 community.

12.3 Sharing nudes and semi-nudes and AI-generated sexual imagery

Any report or discovery involving nude or semi-nude imagery, sexualised deepfakes, "deep nudes" or other AI-generated or digitally altered sexual imagery involving, depicting or appearing to depict a child must be reported immediately to the DSL or DDSL. It must be managed in accordance with current UKCIS and KCSIE guidance, Educ8's Safeguarding & Child Protection Policy and the following requirements:

Staff must not intentionally view, copy, print, forward, share, store, save or distribute the imagery and must not ask a learner to display, share, download or delete it. Staff must not investigate the matter themselves.

If a member of staff has viewed the imagery accidentally or unavoidably, they must not view it again. They must report the circumstances immediately to the DSL or DDSL, who will record the incident and consider any support required by the member of staff.

In exceptional circumstances, the DSL may decide that viewing is necessary and proportionate to safeguard a child. This decision must be based on the DSL's professional judgement and current UKCIS guidance. Viewing should only take place where it is the only practicable way to determine the appropriate safeguarding response, is necessary to support a report or removal request, or is unavoidable because the imagery has already been presented to a member of staff or identified through Educ8's systems.

Where exceptional viewing is authorised, it must normally be undertaken by the DSL or by a member of the safeguarding team acting under formally delegated authority. Another member of staff should be present, although they do not need to view the imagery. The reason for viewing, the authority given, the people present and the actions taken must be recorded on CPOMS. The imagery itself must never be copied, printed, shared, stored, saved or uploaded to CPOMS.

A learner's device must not be searched for imagery unless the search is legally permitted, specifically authorised by the Headteacher and coordinated with the DSL. Any search must be conducted in accordance with current DfE guidance, Educ8's Searching, Screening and Confiscation Policy and applicable safeguarding procedures.

Staff must not delete imagery or instruct a learner to delete it before the DSL has assessed the incident. The DSL will determine whether the device should be secured, whether evidence must be preserved, whether the police, children's social care, CEOP or another agency should be contacted and whether deletion or removal should subsequently be arranged.

The DSL will assess the immediate and ongoing risk to every child involved, including any evidence of coercion, grooming, exploitation, extortion, harmful sexual behaviour, malicious sharing or adult involvement. Suspected adult involvement or immediate risk of significant harm must be considered for urgent referral to the police and/or children's social care.

Learners will not be blamed or shamed for making a report. Their welfare, dignity, wishes, feelings, lived experiences and ongoing safety will be prioritised, and appropriate support will be provided.

AI-generated or digitally altered sexual imagery will be treated as potentially harmful and abusive even where no original sexual photograph exists. The fact that imagery is artificial, altered or presented as a joke does not reduce the requirement for an immediate safeguarding assessment.

All decisions, actions and reasons must be recorded on CPOMS without attaching or reproducing the imagery.

12.4 Cyberbullying and online harassment

Cyberbullying, discriminatory abuse, sexual harassment, threats, impersonation, exclusion and other harmful online behaviour will not be tolerated. Reports will be recorded, investigated and responded to under safeguarding, behaviour and anti-bullying arrangements as appropriate.

Affected learners will be supported and advised not to retaliate.

Evidence may be preserved through authorised screenshots, system logs or reports without unnecessarily reproducing harmful or illegal content.

Content may be reported to the platform or service provider and removal requested.

Parents and carers will normally be informed and involved unless doing so would place a child at increased risk of harm, compromise a safeguarding enquiry or investigation, or otherwise be contrary to safeguarding advice.

Police or other agencies will be contacted where a criminal offence or significant risk is suspected.

12.5 Cyber incidents and personal-data breaches

On notification of a suspected cyber incident, IT support and the Headteacher will activate the incident response plan, contain the risk, preserve information, assess impact and inform the DSL, DPO, Headteacher, Executive Board, insurer and external bodies as required.

The DPO will determine whether a personal-data breach has occurred and whether notification to the Information Commissioner's Office or affected individuals is required. Cyber incidents and near misses will be recorded and reviewed to identify lessons and required improvements.

12.6 Concerns or allegations about adults

Technology misuse by an adult may constitute a safeguarding allegation, low-level concern, disciplinary matter, data breach, criminal offence or a combination of these. It must not be managed solely as an IT or general complaint.

Concerns will be handled under the Safeguarding and Child Protection Policy, Staff Behaviour or Code of Conduct, Low-Level Concerns arrangements and KCSIE. The appropriate person will consider LADO consultation or referral and any duty to report to the DBS, Teaching Regulation Agency, police or another body.

12.7 Complaints

Complaints about online safety or technology use will be handled under the Complaints Procedure only after immediate safeguarding, technical-security and data-protection risks have been addressed. The complaints process must not delay a referral or protective action.

12.8 Sanctions, access restrictions and evidence

Any sanction will be lawful, reasonable, proportionate and consistent with the relevant Behaviour Policy, staff disciplinary procedure or contractual arrangements. Consideration will be given to intent, impact, age, SEND, vulnerability, prior understanding, repetition and safeguarding context.

Access may be restricted, suspended or withdrawn where necessary to protect users or systems.

Learner devices may be confiscated, searched or retained only in accordance with statutory guidance and Educ8's Behaviour Policy.

Deletion of material will not be required where it may destroy evidence or where police, the DSL, DPO or IT support advise preservation.

Support and education will accompany sanctions where this will reduce future risk.

13. Learning Platforms and Digital Learning Environments

Platforms must be approved before use and configured for the intended user group.

Access will be limited to current authorised users and removed promptly when no longer required.

Messaging, publishing, file-sharing, AI and collaboration functions will be risk assessed and moderated or restricted where appropriate.

Users will comply with copyright, privacy, acceptable use and assessment-integrity requirements.

Staff will monitor learner activity and content within the platform as required by the monitoring strategy. Inappropriate content will be secured, reported and removed where appropriate without compromising evidence or safeguarding action.

External users such as moderators may receive time-limited, minimum-necessary access approved by an authorised leader.

Account closure, transfer, export and retention will be managed in accordance with contractual and data-protection requirements.

14. Communication and Engagement

14.1 Learners

The policy and learner AUP will be explained in accessible, age-appropriate language during induction and reinforced regularly.

Learners will be told how filtering and monitoring work, why they are used and their limitations.

Reporting routes will be visible, accessible and reinforced, including how to seek help when away from school.

Learner voice will be used to understand emerging platforms, workarounds, barriers to reporting and curriculum needs.

14.2 Staff, volunteers and contractors

Relevant adults will receive this policy or an appropriate summary and must accept the applicable AUP or access conditions.

Induction will explain safeguarding and technical reporting routes, mobile device expectations, professional communication and filtering and monitoring responsibilities.

Updates will be issued whenever risks, systems, guidance or procedures materially change.

14.3 Parents and carers

The policy or an accessible summary will be made available to parents and carers.

Educ8 will explain its mobile phone-free arrangements, learner AUP, filtering and monitoring, reporting routes and expectations for home or remote use.

Information and practical guidance will be shared through appropriate channels and parents encouraged to report concerns promptly.

Parents and carers will be consulted where significant changes directly affect learners or family arrangements, where appropriate.

15. Monitoring and Metrics

Educ8 will use proportionate quantitative and qualitative information to evaluate the effectiveness of this policy and its filtering and monitoring arrangements.

Headteachers, school DSLs and DDSs and IT support will review relevant information arising from their existing systems and procedures. The Head of Safeguarding & Awarding Organisation Compliance will consider group-wide safeguarding themes, patterns and emerging risks.

Monitoring will focus on:

significant or recurring online safety incidents and safeguarding concerns;

high-risk monitoring alerts and whether they were reviewed and acted upon promptly;

filtering or monitoring failures, attempts to bypass controls and periods of reduced protection;

evidence that required technical checks and the annual filtering and monitoring review have been completed;

the effect of filtering arrangements on safeguarding, teaching and learning, including any significant over-blocking;

completion of relevant staff training and Acceptable Use Agreements;

learner understanding and learner voice where relevant;

significant cyber incidents, personal data breaches or complaints; and

identified risks, agreed actions and whether those actions have been completed.

Information will be drawn from existing sources wherever possible, including CPOMS, filtering and monitoring reports, IT support records, risk assessments, training records and governance reports. A separate record or report will not be created where the required evidence is already held securely within an approved system.

A summary of effectiveness, significant risks and outstanding actions will be reported at least annually through the agreed governance arrangements to the Portfolio Director – Education, Safeguarding & Standards, the Executive Board and the individual proprietor or joint proprietors of each school.

Serious safeguarding concerns, material filtering or monitoring failures, significant cyber incidents and personal data breaches must be reported and escalated without delay and must not be held until the next scheduled report.

Monitoring information will be presented in a form that protects confidentiality and will be used to improve safeguarding practice, technical controls, staff training, learner education and risk management

16. Quality Records

Required record	Custodian
Policy approval and revision record	Document owner / Executive Board
Online safety risk assessment and associated actions	Headteacher / school DSL
Annual filtering and monitoring review, including identified gaps and agreed actions	Head of Safeguarding & Awarding Organisation Compliance, with contributions from Headteachers, school DSLs or DDSLs, IT support and the Portfolio Director – Education, Safeguarding & Standards
Evidence of relevant filtering and monitoring checks and technical actions	IT support
Safeguarding concerns, decisions, referrals and outcomes	School DSL or DDSL through CPOMS
Significant cyber incidents, system failures and near misses	IT support / Headteacher
Data protection impact assessments and personal data-breach records, where required	Data Protection Officer
Staff training and Acceptable Use Agreement records	HR / Headteacher
Learner and visitor Acceptable Use Agreement records	Headteacher / school administration
Governance assurance and evidence of completed improvement actions	Relevant document or action owner / Executive Board

An Educ8-wide annual filtering and monitoring review may be used, provided that the review clearly considers and records the particular risks, arrangements, findings and required actions for each school.

Records already held within CPOMS, filtering and monitoring systems, IT support records, HR records or approved governance records will constitute the required evidence. Information must not be duplicated solely to create an additional quality record.

Records will be retained and securely disposed of in accordance with Educ8's records retention schedule, safeguarding requirements and data protection obligations. Access will be restricted to those with a legitimate need to know.

Where a technical alert relates to a safeguarding concern, the relevant facts, decisions and actions must be recorded on CPOMS. Technical reporting does not replace the safeguarding record.

Nude or semi-nude imagery, sexualised deepfakes, "deep nudes" or other AI-generated or digitally altered sexual imagery involving or appearing to involve a child must never be copied or attached to CPOMS or any other Educ8 record.

17. Forms and Templates

Reference	Title
Appendix 1	Information, Advice and Support
Appendix 2	Visitor and Contractor Acceptable Use Conditions
Appendix 3	Staff Acceptable Use Agreement
Appendix 4	Filtering and Monitoring Minimum Review Schedule
Internal record	Online Safety Risk Assessment and Action Plan
Internal record	Filtering and Monitoring Annual Review and Check Log
Internal record	Approved Digital and AI Services Register
D0012IT	Learner Acceptable Use & Online Safety Agreement
F0014SA	Safeguarding Induction and Annual Declaration
External	360 Safe or equivalent online safety self-review tool

Appendix 1 - Information, Advice and Support

The following current sources should be used in preference to static or historic platform-specific advice. Links should be checked as part of the annual policy review.

- [Keeping Children Safe in Education](#)
- [DfE Filtering and Monitoring Core Standard](#)
- [DfE Cyber Security Core Standard](#)
- [DfE Generative AI in Education](#)
- [DfE Mobile Phones in Schools](#)
- [DfE RSHE statutory guidance](#)
- [CEOP Education and Safety Centre](#)
- [Childline](#)
- [Internet Watch Foundation](#)
- [UK Safer Internet Centre](#)
- [Internet Matters](#)
- [NSPCC Online Safety](#)
- [Educate Against Hate](#)
- [360 Safe](#)
- [SWGfL Test Filtering](#)
- [National Cyber Security Centre](#)
- [Report Fraud](#)

Appendix 2 - Visitor and Contractor Acceptable Use Conditions

A visitor or contractor granted access to Educ8 technology, networks or information must:

- use only the access, device and information specifically authorised for the agreed purpose;
- keep any account or access code confidential and not allow another person to use it;
- use the designated guest or contractor network and not connect unauthorised equipment;
- not bypass security, filtering or monitoring or install software, applications or extensions;
- protect personal and confidential information and comply with applicable contractual and data-protection requirements;
- not photograph, film, record or communicate with learners unless specifically authorised;
- report safeguarding concerns immediately to a member of Educ8 staff and technical or security concerns to their Educ8 contact; and
- understand that access may be monitored, restricted or withdrawn.

Acceptance may be recorded through a signed agreement, contract, induction record, visitor sign-in process or electronic acknowledgement, according to the level of access provided.

Appendix 3 - Staff Acceptable Use Agreement

I confirm that I have read and understood the Acceptable Use of Technology and Online Safety Policy and agree that I will:

- Use Educ8 technology, accounts and information only for authorised and lawful purposes.
- Maintain professional boundaries and use only approved channels to communicate with learners.
- Protect credentials, use multi-factor authentication where provided and report suspected compromise immediately.
- Use only authorised devices, storage, applications, extensions, AI services and communication platforms.
- Not store learner or Educ8 information on personal devices or personal accounts.
- Not enter identifiable, safeguarding, confidential or special-category information into an unauthorised AI service.
- Critically verify AI output and remain professionally accountable for final work.
- Actively supervise learners using technology and report unsuitable content, system failures, circumvention attempts or unreasonable over-blocking.
- Report safeguarding concerns to the DSL and not rely on reporting them solely to IT support.
- Report cyber incidents to IT support and data breaches to the DPO immediately.
- Not photograph, film or record learners on a personal device.
- Maintain appropriate personal social-media privacy and not connect personally with current learners.
- Understand that proportionate authorised monitoring may occur.
- Preserve evidence and confidentiality and not undertake unauthorised investigations.

Appendix 4 - Filtering and Monitoring Minimum Review Schedule

Frequency	Minimum activity	Lead/involvement	Required record
Continuous / immediate	High-risk alerts; reported safeguarding concerns; filtering failures; cyber incidents; personal-data breaches.	DSL / IT support / SLT lead / DPO as applicable	Incident record and action/outcome
Weekly	Monitoring report highlighting incidents, trends and actions.	DSL and SLT lead	Reviewed report and actions
Termly	Recorded sample checks across sites, devices, user groups and relevant locations; account and exception review; risk and action-plan review.	IT support with SLT lead and DSL	Check log and action update
Before release or change	New device, service, network, AI tool, filtering profile, monitoring configuration or material system change.	IT support / DPO / DSL / SLT lead	Approval, testing and risk/DPIA record
At least annually	Formal effectiveness review covering all devices, sites, networks, user groups, off-site use, risk profile, incidents, curriculum, AI, blocklists, monitoring, governance and training.	SLT lead supported by DSL and IT; responsible Director involved	Annual review and Board assurance
After a significant incident	Effectiveness of controls, response, reporting, evidence, training and required changes.	Relevant leads	Post-incident review and lessons learned

Each recorded check must state the date, person completing it, devices or systems checked, location and user profile, test undertaken, result, required action, owner, target date and completion evidence.