



LIGHTHOUSE

LEARNING PROVISION

— BELONG • GROW • ACHIEVE • THRIVE —

— PRACTICAL LEARNING. EMOTIONAL GROWTH. PREPARATION FOR ADULTHOOD. —

OPERATIONAL AND PUBLIC POLICY

Online Safety and Acceptable Use Policy

Belong • Grow • Achieve • Thrive

Organisation	Lighthouse Learning Provision Ltd
Policy owner	Board of Directors / Designated Safeguarding Lead
Online Safety Lead	Adam Waldron - Director and Designated Safeguarding Lead
Deputy / Data Protection Lead	Rachel Waldron - Director, Deputy DSL and Named Safeguarding Person
Approved / published	July 2026 Version 2.0
Review	July 2027, or sooner following relevant legal, safeguarding, technological, operational or commissioning change

Technology must be used to extend opportunity without weakening safeguarding, privacy, professional boundaries or the dignity of any learner.

Contents

1. Purpose and aims
2. Scope, status and legal framework
3. Online safety principles and the four areas of risk
4. Roles, responsibilities and governance
5. Risk assessment and learner-specific planning
6. Authorising learner access and acceptable use
7. Online safety education and digital resilience
8. Learner devices, mobile phones, smart watches and wearables
9. Professional communication, social media and staff boundaries
10. Filtering, monitoring and technical safeguards
11. Artificial intelligence and emerging technology
12. Images, video, audio and learner work
13. Sharing nudes or semi-nudes and image-based abuse
14. Cyberbullying, harassment and discriminatory harm
15. Grooming, exploitation, radicalisation, self-harm and harmful content
16. Gaming, gambling-like features, scams and commercial risk
17. Remote learning, video calls and online meetings
18. Data protection, cyber security and information ownership
19. Responding to online safety incidents
20. Concerns about adults, allegations and low-level concerns
21. Partnership with parents, carers, schools and commissioners
22. Complaints, consequences and restorative responses
23. Training, assurance, monitoring and review
24. Reference framework

Policy at a glance

Online safety is both a safeguarding responsibility and an essential life skill. Lighthouse will combine active supervision, learner education, secure systems, proportionate technical controls and clear professional boundaries. No filter or monitoring product replaces trusted relationships, professional curiosity or prompt safeguarding action.

1. Purpose and aims

1.1 This policy establishes how Lighthouse Learning Provision Ltd enables safe, purposeful and responsible use of digital technology while protecting children, adults, information and organisational systems from online harm.

1.2 Lighthouse will:

- use technology to support personalised learning, creativity, communication, independence and preparation for adulthood;
- help learners develop critical thinking, consent, digital citizenship, resilience and help-seeking skills;
- identify and manage risks arising from content, contact, conduct and commerce;
- maintain clear boundaries for staff communication, images, social media and personal devices;
- provide proportionate filtering, monitoring, cyber security and data-protection controls;
- respond promptly to online safeguarding concerns and preserve evidence safely; and
- work with families, schools, Local Authorities, police, social care and specialist services where required.

1.3 The policy is intended to support safe opportunity rather than simply prohibit technology. Restrictions must have a clear purpose, be proportionate to assessed risk and be reviewed.

2. Scope, status and legal framework

2.1 Lighthouse is an independent non-school alternative provision provider. It adopts relevant school-sector online-safety expectations as good practice, but does not claim statutory powers that apply only to schools or colleges.

2.2 This policy applies to directors, employees, self-employed practitioners, contractors, agency workers, volunteers, visitors and learners. It covers organisation-owned and personal devices used in connection with Lighthouse, including phones, tablets, laptops, smart watches, cameras, cloud systems, email, messaging, social media, games, artificial intelligence tools, remote learning, images and recordings.

2.3 It applies at the base, during transport, community and outdoor learning, off-site activities, outreach, remote sessions, staff home working and any work-related communication.

2.4 The policy is informed by Working Together to Safeguard Children 2026, current local safeguarding procedures, the voluntary national standards for non-school alternative provision, relevant principles in Keeping Children Safe in Education, data-protection law, the Computer Misuse Act 1990, the Online Safety Act 2023 and current DfE, UKCIS, ICO and NCSC guidance.

2.5 KCSIE 2025 remains the current school and college guidance until 31 August 2026; KCSIE 2026 applies from 1 September 2026. Lighthouse will apply the current edition relevant to the date of operation.

3. Online safety principles and the four areas of risk

3.1 Lighthouse recognises that online and offline safeguarding are inseparable. Technology may extend or intensify abuse, exploitation, bullying, coercion, discrimination, self-harm risk and criminal activity.

Area	Examples
Content	Pornography; violent or hateful material; racism, misogyny or discrimination; self-harm and suicide content; extremist material; misinformation, disinformation, conspiracy content, deepfakes and harmful AI-generated material.
Contact	Grooming; adults or peers seeking sexual, criminal or financial exploitation; coercive contact; stalking; unwanted communication; unsafe communities; impersonation and social engineering.
Conduct	Cyberbullying; harassment; sharing images; abusive messages; online conflict; illegal or risky posting; hacking; creating harmful content; misuse of AI; damage to another person's privacy or reputation.
Commerce	Scams; phishing; fraud; gambling and loot boxes; in-app purchasing; subscription traps; inappropriate advertising; financial exploitation; counterfeit or illegal goods.

3.2 Decisions will be guided by the child's best interests, age, development, SEND, communication needs, lived experience, vulnerability, current risk and ability to use technology safely with support.

3.3 Adults will maintain an attitude of "it could happen here", avoid assuming that a learner is safe because they appear technically skilled, and recognise that children may not understand that an online experience is abusive or exploitative.

4. Roles, responsibilities and governance

4.1 Board of Directors

- sets the organisational approach to online safety and provides sufficient resources, competent advice and secure systems;
- ensures filtering, monitoring and cyber-security arrangements are proportionate to Lighthouse's actual technology and learner risks;
- approves online platforms, communication routes, AI tools and significant changes to digital systems;
- reviews serious incidents, patterns, technical alerts, complaints, data breaches and improvement actions;
- ensures commissioners receive accurate information about Lighthouse's controls and any material change; and
- confirms that no learner receives internet or platform access before required controls are operational and tested.

4.2 Adam Waldron - Director, DSL and Online Safety Lead

- leads safeguarding responses to online concerns and coordinates referrals or police contact;
- maintains oversight of learner online-safety risk assessments and incident records;
- ensures staff understand the four areas of online risk and the operation of filtering and monitoring;
- reviews alerts, patterns and learner feedback with appropriate technical support;
- approves or escalates decisions about device access, images, remote contact and online communication; and
- reports assurance and improvement needs to the Board.

4.3 Rachel Waldron - Director, Deputy DSL and Data Protection Lead

- provides safeguarding cover and leads where a concern involves the DSL;
- advises on privacy, lawful processing, supplier due diligence, data sharing and data breaches;
- supports review of AI tools, cloud services, images, consent and records; and
- has authority to suspend access or contact statutory services where risk requires immediate action.

4.4 All adults

- use only authorised systems and channels for work involving learners;
- supervise according to risk and actively engage rather than relying on technical controls;
- protect passwords, devices and confidential information;

- model respectful, balanced and lawful use of technology;
- report harmful content, contact, behaviour, technical alerts, boundary concerns and cyber incidents immediately;
- do not investigate safeguarding matters or obtain evidence unlawfully; and
- self-report accidental contact, image retention, misdirected communication or any situation that could be misunderstood.

4.5 Learners

Learners will be supported to understand and follow an accessible acceptable-use agreement. A learner's additional needs, developmental stage or previous harmful experiences will be considered when explaining expectations and responding to incidents.

5. Risk assessment and learner-specific planning

5.1 Online safety will form part of referral, admission and ongoing risk assessment. Relevant information should include device access, social-media use, online relationships, exploitation, bullying, self-harm content, sexual imagery, gaming, spending, radicalisation, missing episodes, previous restrictions and protective factors.

5.2 Individual plans may address:

- which devices and networks may be used and for what purpose;
- level and proximity of supervision;
- whether headphones, cameras, messaging, gaming, social media or AI tools are permitted;
- known contacts, apps, keywords, content or patterns requiring additional vigilance;
- safe storage of devices during activities;
- agreed responses to distressing content, contact or attempts to leave supervision;
- family and commissioner communication arrangements; and
- how restrictions will be reviewed and reduced when safe.

5.3 Risk assessment must not become a substitute for education or relationship-based support. Learners should be helped to understand risk and develop safer choices wherever possible.

6. Authorising learner access and acceptable use

6.1 Internet, platform and device access must be authorised as part of the placement or session arrangements. The purpose, supervision and relevant expectations must be clear to the learner.

6.2 Learners are expected to:

- use technology for the agreed learning, communication or wellbeing purpose;
- treat other people respectfully and not create, seek, share or encourage harmful content;
- protect passwords and personal information and not use another person's account;
- tell an adult if content or contact makes them worried, pressured, ashamed, unsafe or uncomfortable;
- not bypass filtering, install unauthorised software, alter settings, access another person's data or attempt hacking;
- ask before photographing, recording or sharing information about another person; and
- return or place devices in the agreed location when requested for safety or learning reasons.

6.3 Access may be adapted or temporarily restricted where there is a clear safeguarding, privacy, cyber-security or significant disruption risk. The learner will be told the reason in an accessible way, provided with an alternative where practicable and given a review point.

7. Online safety education and digital resilience

7.1 Online safety learning will be age-, development- and need-appropriate and may be delivered through practical projects, emotional literacy, life skills, individual work, discussion, scenario work or targeted intervention.

7.2 Evaluating information and content

- distinguishing fact, opinion, advertising, satire, edited material and deliberate deception;
- checking sources, authorship, dates, evidence, motives and corroboration;
- recognising deepfakes, manipulated images, AI-generated content and false authority;
- understanding cookies, profiling, recommendation systems and digital footprints; and
- questioning why someone wants information, attention, money, belief or action.

7.3 Persuasion and manipulation

- grooming, coercion, flattery, threats, secrecy, debt and reward;
- misinformation, conspiracy narratives and polarising content;
- persuasive design, notifications, streaks, autoplay, loot boxes and pressure to remain online;

- social engineering, phishing, fake identities and scams; and
- commercial and influencer content that is not clearly presented as advertising.

7.4 Online behaviour and relationships

- the same expectations of dignity, consent, honesty and respect apply online and offline;
- anonymity, distance and group dynamics can intensify harmful behaviour;
- banter, misogyny, racism, homophobia, ableism and humiliation are not normalised;
- strategies for disengaging, blocking, reporting, preserving evidence and seeking help; and
- repairing harm without pressuring a harmed child into unsafe mediation.

7.5 Seeking support

Learners will be helped to identify trusted adults, internal reporting routes, platform reporting tools and specialist services such as Childline, CEOP and Report Remove where relevant. Reporting will be praised and never treated as creating a problem.

8. Learner devices, mobile phones, smart watches and wearables

8.1 Personal devices may be brought only under the agreed placement and site arrangements. Lighthouse may require devices to be switched off, placed in a secure agreed location or used only under supervision.

8.2 Decisions will consider the device's role in safety, communication, medical needs, transport and emotional regulation. A device will not be removed in a way that leaves a learner without a necessary emergency or accessibility arrangement unless a safe alternative is provided.

8.3 Personal mobile data, hotspots, smart watches and app-based communication may bypass Lighthouse filtering. Where these are permitted, supervision and individual risk controls must address that limitation.

8.4 Lighthouse does not have the statutory search powers of a school. Staff will not compel a learner to unlock a personal device or conduct intrusive searches. Where serious harm, illegal content, weapons, exploitation or a crime is suspected, the device should be preserved without unnecessary access and the DSL, parent or carer, commissioner and police consulted according to risk.

9. Professional communication, social media and staff boundaries

9.1 Adults must not communicate with learners through personal social-media accounts, personal email, personal gaming accounts, disappearing-message services or secret or unmonitored channels.

9.2 Adults must not search for, follow, befriend, subscribe to or interact with learners or their families through personal accounts. Existing family or community connections must be declared and managed transparently.

9.3 Work communication must use Director-approved channels, have a clear professional purpose, use appropriate language and recipients, and occur at reasonable times unless an emergency arrangement applies.

9.4 Staff-only messaging groups may be used only when authorised. Directors must retain administrative oversight where possible. Sensitive learner information should be kept to the minimum necessary and moved to the approved case or record system. Learners and family members must not be added to staff-only groups.

9.5 Unsolicited messages, friend requests, images or inappropriate contact must not be deleted reflexively. The adult should avoid engaging, preserve the minimum necessary information, report it to the DSL or Director and follow advice.

9.6 Adults should consider how public posts, comments, images, usernames and group membership could affect professional credibility, confidentiality and trust. Privacy settings reduce but do not remove this risk.

10. Filtering, monitoring and technical safeguards

10.1 Before learners use Lighthouse-managed internet, devices or accounts, suitable filtering, monitoring, account management and security controls must be configured, documented and tested.

10.2 Lighthouse will apply the following principles:

- filtering should block harmful and inappropriate content without unreasonably restricting learning;
- monitoring should identify and alert appropriate adults to activity associated with content, contact, conduct and commerce risks;
- roles for technical administration, safeguarding review and escalation must be clear;
- systems must reflect learner age, SEND, risk profiles, managed devices, mobile or app use and artificial intelligence;
- alerts must be reviewed by a competent person and not left solely to automated decision-making;
- monitoring must be lawful, transparent and proportionate, with privacy information provided;
- staff must understand what is and is not monitored and how to report concerns; and

- technical controls must be reviewed at least annually and checked after significant changes, incidents or evidence of ineffective operation.

10.3 Filtering and monitoring cannot identify every risk, particularly on personal mobile data, encrypted services, offline sharing or new platforms. Active supervision, learner education and professional curiosity remain essential.

10.4 Attempts to bypass controls, repeated blocked searches, unusual downloads, malware or high-risk alerts will be reviewed in context and may be both a safeguarding concern and a cyber-security incident.

11. Artificial intelligence and emerging technology

11.1 Generative AI and other emerging technologies may support creativity, accessibility, planning and learning, but they can also create inaccurate, biased, manipulative, sexual, violent, extremist or unsafe outputs and may expose personal information.

11.2 AI tools may be used only where authorised for the specific purpose and user group. Assessment will consider intended purpose, age suitability, terms of use, privacy, data location, security, filtering, administrator controls, output risks, intellectual property, accessibility and safeguarding.

11.3 Adults and learners must not enter names, safeguarding information, health information, images, identifiable learner work or other confidential data into public or unapproved AI tools.

11.4 AI outputs must be treated as generated material rather than fact. Important information must be checked against reliable sources. AI must not be used as a substitute for professional safeguarding judgement, diagnosis, assessment or human decision-making.

11.5 Prohibited uses include generating or altering sexual images of children, “nudification”, impersonation, humiliating deepfakes, harmful instructions, discriminatory material, malware, deception or content intended to threaten or exploit another person.

11.6 Where AI supports learner work, staff will agree how its use is acknowledged and how the learner’s own understanding and contribution are evidenced.

12. Images, video, audio and learner work

12.1 Images and recordings may be created only for an identified educational, safeguarding, evidence, communication or promotional purpose, with a lawful basis and consent where required. Public use requires specific authorisation and must not reveal unnecessary identifying or location information.

12.2 Lighthouse’s preferred practice is to use organisation-owned equipment. Where no suitable organisation device is available, a Director or DSL may authorise temporary use of a personal device for a specific purpose, provided that:

- the purpose and parental or commissioner permissions are confirmed;
- the image is not taken through a personal social-media or messaging app;
- automatic personal cloud backup is disabled or the image is removed from it;
- the image is transferred to approved Lighthouse storage as soon as reasonably practicable;
- the original and all local or cloud copies are permanently deleted immediately after verified transfer; and
- any inability to transfer or delete, accidental upload or unauthorised access is reported immediately as a safeguarding and data-protection incident.

12.3 Adults must not retain learner images for personal portfolios, private records or future use. Learners must not photograph or record others without permission.

13. Sharing nudes or semi-nudes and image-based abuse

13.1 Any incident involving nude or semi-nude images, sexual livestreams, sexualised deepfakes, coercion, threats to share images or image-based abuse must be reported immediately to the DSL or Deputy DSL.

13.2 Staff must not:

- ask a learner to send or show the image again;
- view the image unless unavoidable and specifically necessary for safeguarding decision-making;
- copy, print, save, forward, screenshot, upload or share the image;
- delete content before the DSL or police has advised where evidence may be required; or
- blame, shame or punish a child simply for having created or shared an image.

13.3 The DSL will follow current UKCIS guidance, assess coercion, age, power imbalance, distribution, adult involvement, exploitation, immediate risk and police or social-care thresholds. Parents and commissioners will be involved unless doing so would increase risk or conflict with statutory advice.

13.4 Learners may be supported to use appropriate reporting and removal routes, including platform reporting, CEOP and Childline/IWF Report Remove.

14. Cyberbullying, harassment and discriminatory harm

14.1 Cyberbullying may be repeated or a single act capable of wide or lasting harm. It includes abusive messages, exclusion, impersonation, rumours, doxxing, threats, humiliation, hate content, non-consensual images and coordinated group behaviour.

14.2 Online racism, misogyny, sexism, homophobia, biphobia, transphobia, ableism, faith-based abuse and other discriminatory harm will be challenged and managed through safeguarding, anti-bullying and equality procedures.

14.3 The harmed learner will be protected and supported. The learner displaying harmful behaviour will receive proportionate safeguarding assessment, education, accountability and support. Restorative work will occur only where safe, voluntary and not used to minimise abuse.

15. Grooming, exploitation, radicalisation, self-harm and harmful content

15.1 Online contact may be used to groom a child for sexual, criminal, financial, ideological or other exploitation. Warning signs may include secrecy, new devices or accounts, unexplained money, gifts, threats, debt, older contacts, repeated absence, sexualised communication, pressure to move platforms or fear of losing access.

15.2 Concerns about radicalisation, extremist communities, violent ideology, terrorism-related material or credible threats will be managed as safeguarding matters and referred through Prevent, police or emergency routes as appropriate.

15.3 Content promoting self-harm, suicide, eating disorders, dangerous challenges, weapons or violence may indicate immediate risk. Staff must not leave a learner at immediate risk alone, should obtain emergency health or police assistance where required and must preserve relevant information safely.

15.4 Misinformation and conspiracy material will be addressed through curiosity, evidence, trusted relationships and critical thinking. Staff will avoid humiliating or escalating a learner while maintaining clear safeguarding boundaries.

16. Gaming, gambling-like features, scams and commercial risk

16.1 Learners will be helped to understand gaming communities, voice and text chat, age ratings, live streaming, virtual currencies, loot boxes, skin betting, gambling-like mechanics, spending pressure and contact from strangers.

16.2 Lighthouse devices and accounts must not be used for gambling, unauthorised purchases, cryptocurrency trading, betting, purchasing illegal goods or accessing age-restricted services.

16.3 Suspected scams, phishing, account compromise, financial exploitation or unauthorised transactions must be reported promptly. Staff should not shame the learner or attempt private repayment arrangements with a suspected offender.

17. Remote learning, video calls and online meetings

17.1 Remote sessions require an approved platform, identified participants, agreed times, emergency contacts, professional settings, privacy controls and a clear safeguarding plan.

17.2 One-to-one remote contact must be risk assessed, authorised and recorded. A parent, carer, commissioner or second adult may be included or made aware where this is necessary for safeguarding.

17.3 Adults must use professional accounts, appropriate backgrounds and language, ensure conversations cannot be overheard by unauthorised people and end the session if identity, safety or privacy cannot be maintained.

17.4 Sessions must not be recorded unless there is a specific purpose, lawful basis, prior agreement, secure storage plan and clear retention period.

18. Data protection, cyber security and information ownership

18.1 All personal information, learning records, photographs, messages and work created or processed for Lighthouse remain subject to the Data Protection Policy, contractual confidentiality and organisational ownership requirements.

18.2 Adults must:

- use strong unique passwords and multi-factor authentication where available;
- lock screens and devices when unattended;

- install updates and security patches promptly on authorised devices;
- not share accounts or credentials;
- avoid unapproved removable media, software, cloud storage and browser extensions;
- verify recipients before sending sensitive information and use blind copy appropriately;
- not place learner names or sensitive details in email subject lines;
- report phishing, malware, loss, misdirection, hacking or unauthorised access immediately; and
- avoid confidential conversations or visible records in public or shared environments.

18.3 Cyber incidents will be contained, logged and assessed for safeguarding, operational and personal-data-breach implications. Where required, relevant authorities, commissioners, insurers and affected people will be notified.

19. Responding to online safety incidents

Immediate response

Stay calm. Secure immediate safety. Do not promise secrecy. Do not forward harmful or illegal content. Preserve the minimum necessary evidence. Report to Adam Waldron (DSL) or Rachel Waldron (Deputy DSL) immediately. Call 999 where there is immediate danger, serious injury, a crime in progress or an urgent threat.

19.1 The receiving adult should:

- listen and take the learner seriously;
- establish only the minimum facts needed for immediate safety;
- record what was seen, heard or reported, including usernames, platform, time, URL or account details where safely available;
- avoid confronting an alleged offender or alerting them where this could increase risk;
- avoid deleting, forwarding, copying or extensively viewing content;
- preserve devices or accounts without conducting an unauthorised investigation;
- report verbally to the DSL without delay and complete the incident record; and
- continue supporting the learner and follow any emergency or safeguarding plan.

19.2 The DSL will assess immediate danger, safeguarding thresholds, police or social-care referral, commissioner and family communication, evidence preservation, platform reporting, content removal, technical containment and changes to the learner's risk and support plan.

19.3 A technical or behavioural incident must not be treated only as misuse if it may reveal abuse, exploitation, distress, unmet need or a pattern of harm.

20. Concerns about adults, allegations and low-level concerns

20.1 Any concern that an adult has used technology to harm a child, communicate secretly, access or create sexual content, breach professional boundaries, photograph without authority, misuse information or behave in a way indicating risk or unsuitability must be reported immediately under the Safeguarding and Child Protection Policy.

20.2 A concern about Adam Waldron must be reported to Rachel Waldron. A concern about Rachel Waldron must be reported to Adam Waldron. Where both are implicated or internal reporting is unsafe, the concern must be raised directly with the relevant LADO, commissioner, police, children's social care or NSPCC Whistleblowing Advice Line.

20.3 Potential evidence must be preserved and no internal investigation should compromise LADO, police or social-care processes. Low-level concerns, including over-familiar messaging, unnecessary contact, personal-device images or inappropriate online interaction, must also be recorded and reviewed for patterns.

21. Partnership with parents, carers, schools and commissioners

21.1 Lighthouse will explain its technology and device arrangements during referral and induction and provide this policy and acceptable-use expectations in accessible formats.

21.2 Commissioners and families should share relevant online-safety information, current restrictions, known contacts, harmful incidents, device arrangements and risk plans. Material concerns will be communicated without delay through the agreed safeguarding route.

21.3 Lighthouse will work with families to build balanced understanding of online opportunities and risks. A safeguarding concern will not be withheld or delayed because a family or commissioner has not yet been contacted.

21.4 Where a learner uses a commissioner-owned device or platform, the commissioner's filtering, monitoring, account and incident-response responsibilities must be agreed. Lighthouse will not assume that another organisation's controls apply at the Lighthouse site without confirmation.

22. Complaints, consequences and restorative responses

22.1 Complaints about online safety, privacy, communication or technology are handled under the Complaints Policy. Safeguarding concerns, allegations and data breaches are transferred immediately to the relevant procedure and are not delayed by complaint stages.

22.2 Responses to learner misuse will be proportionate, educational and sensitive to SEND, trauma, intent, impact, repetition, coercion and safeguarding context. Possible responses include additional teaching, supervision, temporary access changes, support plans, restorative work where safe, commissioner review or external referral.

22.3 Serious or deliberate staff misuse may lead to contractual, disciplinary, safeguarding, LADO, DBS, police or regulatory action. A genuine mistake reported promptly will be addressed fairly but still recorded and risk managed.

23. Training, assurance, monitoring and review

23.1 All adults will receive induction and updates covering:

- the four areas of online risk and emerging harms;
- professional communication, personal devices, images and social media;
- how Lighthouse filtering and monitoring operates and each person's role;
- sharing nudes and semi-nudes, grooming, cyberbullying, exploitation and harmful content;
- AI, deepfakes, misinformation, data protection and cyber security;
- responding to disclosures, preserving evidence and making referrals; and
- learner-specific online-safety risks relevant to the adult's role.

23.2 The Online Safety Lead and Data Protection Lead will review incidents, alerts, blocked activity, device concerns, complaints, learner voice, technical performance, staff training and commissioner feedback for patterns and improvement.

23.3 Filtering and monitoring arrangements will receive a formal review at least annually and practical checks after system changes, serious incidents or evidence of bypass or failure. The review will consider learner risk profiles, including generative AI use.

23.4 This policy is reviewed at least annually and sooner after a serious incident, significant technology change, new site or service, commissioner requirement or legal or guidance change.

24. Reference framework

External framework

- Keeping Children Safe in Education 2025 and 2026 - relevant online-safety expectations adopted as good practice
- Working Together to Safeguard Children 2026
- Non-school alternative provision: voluntary national standards
- Teaching online safety in schools
- Education for a Connected World - 2020 edition
- Meeting digital and technology standards in schools and colleges - filtering and monitoring and cyber-security standards
- UKCIS Sharing nudes and semi-nudes: advice for education settings
- Generative AI in education and Generative AI product safety standards
- Children and the UK GDPR and the Children's Code - ICO
- Computer Misuse Act 1990 and Online Safety Act 2023
- NCSC cyber-security guidance for education

External guidance and contact routes checked 23 July 2026. Current official guidance takes precedence where a source changes.