



St. Lawrence Church of England
Primary School

ONLINE SAFETY POLICY

SEPTEMBER 2026

Policy Leader and Online Safety Lead: James Davis

Headteacher and Designated Safeguarding Lead: Richard Crook

Data Protection Officer: James Davis

Safeguarding Governor: Dotun Fasanya

Last reviewed on: September 2026

Approved by: Governing Body

Next review on: September 2027

CONTENTS

1. Context and Rationale
2. Aims Scope and Definitions
3. Legislation Guidance and Related Policies
4. Roles and Responsibilities
5. Online Safety Education for Pupils
6. Training for Staff Volunteers and Governors
7. Working with Parents Carers and the Wider Community
8. Technical Security and Access Management
9. Filtering and Monitoring
10. Mobile Smart and Personal Devices
11. Digital Images Video and Audio
12. Communications Social Media and Professional Identity
13. Artificial Intelligence and Emerging Technologies
14. Data Protection Privacy and Records
15. Reporting and Responding to Online Safety Incidents
16. Safeguarding Incidents and Nudes and Semi Nudes
17. Illegal Content and Preserving Evidence
18. Behaviour Consequences and Staff Misconduct
19. Monitoring Review and Governance Assurance
20. Appendix A Immediate Response Guide
21. Appendix B Filtering and Monitoring Review Record

1. CONTEXT AND RATIONALE

The Bible tells us that we are all “children of God” (John 1:12). As such, we consider every member of our school community to be part of our school family - a family that works together to provide a safe, supportive, happy and stimulating environment. An environment that allows children to face the world with resilience, integrity and joy.

Learning together, rooted in God, pupils at St. Lawrence Church of England Primary School are taught to use technology with confidence, curiosity, kindness and good judgement. Digital technology brings significant benefits to learning, communication and participation. It can also expose children and adults to harmful content, contact, conduct and commercial risks. Online safety is therefore an essential part of safeguarding and of the school's culture, curriculum and everyday practice.

This policy sets out the school's whole-school approach to protecting and educating pupils, supporting staff and families, managing technology safely and responding promptly to concerns. Online safety is not solely a technical matter: safeguarding, curriculum, behaviour, data protection, information security and technical controls must work together.

The policy retains the established principles of the school's previous Online Safety Policy while updating roles, reporting arrangements, filtering and monitoring, artificial intelligence, smart devices and links with the school's current policy framework.

2. AIMS SCOPE AND DEFINITIONS

Aims

- protect pupils, staff and the wider school community from online harm while enabling appropriate use of technology for teaching, learning and administration
- ensure that every member of the school community understands their responsibilities and knows how to report a concern
- provide an age-appropriate, progressive online safety curriculum which develops knowledge, critical thinking, digital resilience and respectful behaviour
- maintain proportionate technical safeguards, including effective filtering and monitoring, without unreasonably restricting teaching and learning
- respond to incidents consistently through safeguarding, behaviour, data protection, staff conduct and law-enforcement procedures as appropriate
- review practice in response to incidents, changes in technology, emerging risks and national guidance.

Scope

This policy applies to pupils, employees, governors, volunteers, trainee teachers, placement students, agency and supply staff, visitors, contractors, parents and carers, community users and anyone using school systems or acting on behalf of the school. It applies to school-owned and school-managed networks, accounts, services and devices, whether used on or off site, and to personal technology used on school premises or in connection with school business.

The school may respond to online behaviour outside school where it affects a pupil's education or welfare, threatens another member of the school community, could adversely affect the reputation or orderly running of the school, or is otherwise within the headteacher's lawful powers. Responses will be proportionate and aligned with the Behaviour and Relationships Policy, Anti-Bullying arrangements and safeguarding procedures.

The four areas of online risk

Area	Examples
<u>Content</u>	Illegal, inappropriate or harmful material; pornography; misogyny or misandry; racism; self-harm or suicide content; extremism; misinformation and disinformation; harmful AI-generated content.
<u>Contact</u>	Harmful interaction with adults, other children or generative AI applications; grooming; exploitation; harassment; coercion; impersonation; pressure to share personal information or imagery.
<u>Conduct</u>	Bullying; abuse; threatening or discriminatory behaviour; sharing nudes or semi-nudes; deepfakes; oversharing; unsafe livestreaming; plagiarism; copyright infringement; misuse of accounts or systems.
<u>Commerce</u>	Online gambling; scams; phishing; financial exploitation; inappropriate advertising; in-app purchases; misleading design; risks associated with data collection.

Online risks often overlap and may facilitate harm offline. Children may be victims, witnesses or responsible for harmful behaviour, and they may move between these positions. A child who has caused harm may also need safeguarding support.

3. LEGISLATION GUIDANCE AND RELATED POLICIES

The school will have regard to current legislation, statutory guidance and relevant national standards. This includes, as applicable:

- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children and local safeguarding partnership procedures
- Education and Inspections Act 2006 and Department for Education advice on behaviour, searching, screening and confiscation
- Prevent duty guidance and the Counter-Terrorism and Security Act 2015
- UK General Data Protection Regulation, Data Protection Act 2018 and Data (Use and Access) Act 2025
- Human Rights Act 1998, Equality Act 2010 and relevant communications, computer misuse, copyright and sexual offences legislation
- Department for Education digital and technology standards, including the Filtering and Monitoring Core Standard and Cyber Security Core Standard
- Department for Education guidance on generative artificial intelligence and product safety expectations
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes.

This policy should be read alongside the following school documents:

- Child Protection and Safeguarding Policy
- Behaviour and Relationships Policy
- Anti-Bullying Policy and child-friendly bullying policy
- Data Protection Policy and privacy notices
- Mobile Phones and Smart Devices Policy
- Artificial Intelligence Policy
- Staff Code of Conduct
- Acceptable Use Policy and associated agreements, once approved
- Curriculum, Relationships and Health Education and relevant teaching plans
- Complaints, whistleblowing, disciplinary and information-breach procedures.

Where documents overlap, the more specific procedure will normally govern the operational response. A safeguarding concern must always be managed under the Child Protection and Safeguarding Policy, regardless of the technology involved.

4. ROLES AND RESPONSIBILITIES

Governing Body

- approve this policy and hold leaders to account for its implementation
- ensure that online safety is a running and interrelated theme within safeguarding, curriculum, staff training, behaviour and technology provision
- ensure that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least once every academic year
- identify a responsible governor and a senior leader for filtering and monitoring assurance and ensure responsibilities are clearly allocated
- receive proportionate assurance about incidents, trends, curriculum, staff training, filtering and monitoring, data protection and improvement actions without receiving unnecessary personal data
- ensure that pupils are taught about safeguarding, including online safety, and that appropriate resources are available.

Headteacher and Senior Leaders

- provide a safe culture and ensure that this policy is implemented consistently
- ensure that the DSL, Online Safety Lead, DPO, Computing Lead and technical support work together and have sufficient authority, time, information and training
- scope the school's technology and safeguarding needs; approve systems and documented exceptions; oversee reports and actions
- ensure staff understand reporting routes and receive relevant induction and updates
- manage allegations, low-level concerns, disciplinary matters and serious incidents under the correct procedure
- ensure parents, carers and users are informed about the school's arrangements.

Designated Safeguarding Lead

- lead on safeguarding and online safety and ensure online concerns are assessed in the same way as other safeguarding concerns
- review relevant filtering and monitoring reports and respond to safeguarding alerts, including immediate high-risk alerts
- work with technical support and senior leaders on risks, system reviews, checks and changes
- ensure that incidents are recorded, referred and followed up under safeguarding procedures
- provide governors with assurance that filtering and monitoring are working effectively and are reviewed regularly
- ensure that the needs of vulnerable pupils and children with SEND are considered.

Online Safety Lead and Computing Lead

- coordinate the development and annual review of this policy and support a coherent online safety curriculum
- maintain awareness of emerging technology, risks and guidance and share relevant updates
- support staff, pupils and parents with education and advice
- work with the DSL and technical provider to analyse incidents and identify prevention, training or curriculum actions
- support the annual filtering and monitoring review but not make safeguarding decisions in place of the DSL.

Data Protection Officer

- advise on privacy, lawful processing, transparency, access, retention and security
- advise on and monitor data protection impact assessments for monitoring technologies, online services and AI tools where high risk is likely
- support the management of personal-data breaches and data-subject rights under the Data Protection Policy
- provide independent advice; safeguarding decisions remain with the DSL and senior leaders.

Technical Support Provider

- maintain secure infrastructure, filtering, monitoring, account controls, updates, backups and technical logs within the agreed service
- ensure filtering and monitoring remain active on relevant networks, services and school-managed devices on and off site where technically applicable
- provide intelligible scheduled reports and immediate high-risk alerts through agreed routes
- record and complete actions following checks or concerns and promptly report safeguarding concerns to the DSL
- work with the DSL and SLT on reviews, testing, risk assessment, procurement and changes; never make safeguarding judgements independently
- preserve confidentiality and access monitoring information only as authorised.

All Staff and Volunteers

- read and follow this policy, the Child Protection and Safeguarding Policy, Staff Code of Conduct and applicable Acceptable Use Agreement
- maintain professional communications and use approved school systems
- supervise pupils' use of technology and use checked, age-appropriate resources
- remain alert to online indicators of harm and report concerns immediately through the school's safeguarding route
- report accidental exposure, weaknesses, bypass attempts, lost devices, suspicious messages, data breaches and misuse without delay
- never investigate a safeguarding concern, search a child's device or view, copy, print, forward or save suspected illegal or indecent imagery unless specifically authorised under an appropriate procedure
- model safe, lawful and respectful technology use.

Pupils

- follow the school's online safety rules and their Acceptable Use Agreement
- use school accounts and devices only as authorised and keep passwords private
- treat others respectfully and never create or share harmful, abusive, discriminatory or sexual content
- tell a trusted adult promptly if something online worries, upsets or frightens them or if they make a mistake
- understand that use of school systems may be filtered and monitored for safety and security.

Parents and Carers

- support the school's online safety expectations and discuss safe, respectful use at home
- report concerns to the school and preserve relevant evidence without redistributing harmful material
- understand age restrictions and supervise access to services, devices, games and purchases appropriately
- work with the school where online behaviour outside school affects a child or the school community.

5. ONLINE SAFETY EDUCATION FOR PUPILS

Technical controls cannot remove every risk. Pupils will therefore receive planned, progressive and age-appropriate education that develops knowledge, skills and confidence rather than relying on fear or prohibition. Online safety will be taught through Computing, Relationships and Health Education, PSHE, English and other relevant curriculum areas, and reinforced whenever technology is used.

- how to recognise the four areas of risk and seek help
- privacy, personal information, passwords, location data, digital footprints and reputation
- healthy relationships, consent, respectful communication, cyberbullying, harassment and discrimination
- grooming, exploitation, coercion, scams, phishing and social engineering
- age restrictions, persuasive design, advertising, gambling-like features and in-app purchases
- critical evaluation of sources, misinformation, disinformation, manipulated media, deepfakes and AI outputs
- copyright, attribution, plagiarism and appropriate use of generative AI
- safe use of search, messaging, gaming, social media, live streaming, video and collaborative services
- what filtering and monitoring do, their limitations, and why concerns must still be reported
- how to block, mute, report and preserve appropriate evidence without sharing harmful content further.

Teaching will be inclusive and adapted for age, development, language, SEND, prior experience and vulnerability while maintaining high expectations. Staff will avoid activities that ask pupils to disclose personal experiences publicly or unnecessarily expose them to harmful examples. Planned internet use will normally use resources checked in advance. If unsuitable content appears, staff will stop or minimise exposure, reassure pupils, preserve evidence appropriately and report the matter.

Pupil voice, curriculum review, incident patterns and current risks will be used to evaluate provision. The school will ensure that pupils know several trusted routes for seeking help and understand that they will be listened to and supported.

6. TRAINING FOR STAFF VOLUNTEERS AND GOVERNORS

Online safety forms part of safeguarding induction and regular safeguarding updates. Training will be proportionate to role and will include reporting routes, child-on-child abuse, harmful and illegal content, professional boundaries, data protection, phishing and social engineering, filtering and monitoring, AI-related risks, and response to accidental exposure.

Staff with specific duties - including the DSL and deputies, Online Safety Lead, Computing Lead, DPO, senior leaders and technical support - will receive role-specific development. Governors will receive training sufficient to provide strategic challenge and assurance. Contractors or volunteers who use systems or work with pupils will receive information appropriate to their access and role.

The school will use incidents, audits, system changes and national developments to identify additional training. Staff must seek advice where unsure; reporting a concern promptly is expected and will not be treated as wrongdoing merely because the concern proves unfounded.

7. WORKING WITH PARENTS CARERS AND THE WIDER COMMUNITY

The school recognises the essential role of parents and carers. It will provide clear information through appropriate channels such as the website, newsletters, meetings, workshops and targeted advice. Information may cover current risks, parental controls, age restrictions, online relationships, gaming, AI, devices, reporting routes and sources of support.

Parents and carers will be informed of significant concerns involving their child unless doing so would place a child at increased risk, compromise a police or safeguarding investigation, or conflict with professional advice. The DSL will decide this in line with safeguarding procedures.

Community users and external organisations using school facilities or systems must comply with relevant school requirements. Any external provider delivering online-safety content must be checked as suitable, and delivery remains subject to school oversight.

8. TECHNICAL SECURITY AND ACCESS MANAGEMENT

The school will maintain defence in depth. Filtering and monitoring support, but do not replace, secure configuration, supervision, education and a culture in which concerns are reported.

- individual accounts will be used where appropriate; access will follow least-privilege principles and be removed promptly when no longer required
- passwords must be strong, private and not shared; multi-factor authentication will be used where required by the school's systems or risk assessment
- administrator access will be restricted, identifiable and used only for authorised tasks
- school-managed devices and software will be supported, patched, protected against malware and configured securely
- backups, recovery arrangements, firewall controls and network separation will be maintained in line with technical standards and risk
- guest and unmanaged devices will use appropriately separated and filtered access; personal hotspots must not be used to bypass school controls
- new systems, apps and services will be assessed and approved before use, including safeguarding, privacy, security, age restrictions, accessibility, contractual and curriculum considerations
- removable media and downloads will be controlled through the Acceptable Use Policy and technical arrangements
- suspected compromise, phishing, malware, lost equipment or unauthorised access must be reported immediately.

Users must not attempt to bypass filtering, monitoring, licensing, access or security controls. Staff must not install software, browser extensions or online services for school use without the required approval. Emergency or temporary access changes must follow the documented exception process in section 9.

9. FILTERING AND MONITORING

Principles

Filtering is preventative: it identifies and blocks illegal, inappropriate or potentially harmful content. Monitoring is reactive: it reviews user activity and produces reports or alerts; it does not itself prevent access. Neither can be completely effective, particularly where content is encrypted, dynamic, personalised, embedded in apps or generated in real time by AI. Appropriate supervision, education and reporting remain essential.

Provision and responsibilities

- the Governing Body has overall strategic responsibility and receives assurance that the standards are met
- the Headteacher and nominated senior leader oversee procurement, scope, documented decisions, reports, exceptions and effectiveness
- the DSL leads safeguarding decisions, checks relevant reports and acts on concerns
- technical support maintains systems, carries out checks, supplies understandable reports and promptly escalates concerns
- the DPO advises where monitoring involves personal data, including transparency, access, retention, security and DPIA requirements
- all staff supervise use, respond to what they see and report weaknesses or concerns.

Minimum operating arrangements

- filtering will be active and up to date across school internet connections and relevant school-managed devices, including when taken off site where the chosen technology provides this coverage
- IWF and Counter-Terrorism Internet Referral Unit blocklists will be implemented through an appropriate provider and must not be capable of being disabled by ordinary users
- pupil and staff profiles will have appropriately different access; controls will reflect age, ability, SEND, curriculum needs and the school's risk profile
- the monitoring plan will combine appropriate technical monitoring with active staff supervision
- the school will receive at least weekly monitoring reports highlighting incidents and immediate reports for high-risk malicious, technical or safeguarding activity
- access to monitoring data will be restricted to authorised persons; information will be used only for legitimate safeguarding, security, conduct or legal purposes
- users will be informed that filtering and monitoring are in place through policies, agreements, notices and, where appropriate, device or login messages
- incidents, decisions and actions will be recorded so that outcomes and system effectiveness can be reviewed.

Checks and annual review

The filtering and monitoring provision will be reviewed at least once each academic year by senior leaders, the DSL, technical support and the responsible governor. The review will be recorded and made available to those entitled to inspect it. Additional review will take place following a serious concern, a material change in working practice, introduction of new technology or generative AI, major software or configuration changes, or evidence that controls are ineffective.

Checks will be scheduled according to risk and will confirm that systems remain active and correctly configured across locations, networks, user groups and school-managed devices. Records will state the date, person completing the check, what was tested, the result and resulting actions. New devices and services will be checked before distribution or use.

Exceptions and overblocking

Filtering must not unreasonably impede teaching, learning, safeguarding or administration. A request to allow or block content must be made through the agreed route and record the requester, resource, reason, users, duration and risk. Technical support must not make a safeguarding exception alone. The responsible senior leader must approve the change and the DSL must assess safeguarding implications. Time-limited exceptions will be preferred and reviewed or removed when no longer required. No exception may disable mandatory illegal-content blocklists.

Staff must report both underblocking and overblocking. They must not use personal data connections, proxy services, VPNs or other methods to circumvent school controls.

10. MOBILE SMART AND PERSONAL DEVICES

Detailed rules are set out in the Mobile Phones and Smart Devices Policy. In summary, pupils must not use mobile phones or similar personal devices during the school day except where expressly authorised. Devices must be handed in, stored or managed in accordance with the school's arrangements. Smart watches capable of messaging, recording, photographing or accessing the internet are treated as mobile devices.

Wearable technology capable of recording, photographing, messaging or online access - including smart glasses - is prohibited for pupils on site unless the Headteacher has approved a specific reasonable adjustment or educational use following a documented risk assessment. Staff, visitors and volunteers must follow the Staff Code of Conduct and Mobile Phones and Smart Devices Policy. Personal devices must never be used to photograph, record or store pupil information.

School-managed devices remain subject to school controls wherever used. Personal devices must not connect to internal networks except through an authorised guest or managed arrangement. The school may confiscate, search or examine a device only where lawful, proportionate and carried out under the school's behaviour, safeguarding and searching procedures. Staff must not conduct an informal search of a child's device.

11. DIGITAL IMAGES VIDEO AND AUDIO

Images, video and audio can enrich learning and celebrate achievement but may expose pupils to privacy, safeguarding and reputational risks. The school will use approved devices and systems, respect consent and privacy information, minimise personal information and consider the context in which material will be viewed or shared.

- staff will use school-provided equipment or an explicitly approved system to capture pupil media
- pupils will be taught to seek permission before recording others and to respect withdrawal or refusal
- names and identifying information will not be combined with images more than necessary
- content will not be published or shared beyond the intended audience without an appropriate lawful basis and school approval
- images must not be taken in toilets, changing areas or other situations involving personal or intimate care, except where a specific safeguarding or care procedure lawfully requires documentation by authorised staff
- parents and visitors must follow event-specific instructions; images taken for personal use must not be used to harass, identify or disadvantage a child
- suspected covert recording, image-based abuse, deepfakes or indecent imagery will be treated as a safeguarding concern.

12. COMMUNICATIONS SOCIAL MEDIA AND PROFESSIONAL IDENTITY

Digital communications must be professional, purposeful and conducted through approved school systems. Staff must maintain clear boundaries and must not use personal email, personal social-media accounts or private messaging services to communicate with pupils or store school information, except where an approved emergency or business-continuity arrangement expressly permits it.

- communications must not contain illegal, abusive, discriminatory, threatening, sexual, defamatory or confidential material
- users must check recipients, attachments and permissions before sending or sharing
- staff must not accept current pupils as friends or followers on personal accounts and should use privacy controls while recognising that nothing posted online can be guaranteed private
- official school accounts require Headteacher approval, named administrators, secure access and moderation arrangements
- comments about pupils, colleagues, parents or school business must not breach confidentiality, professional duties or the Staff Code of Conduct
- public online material that raises a safeguarding, security or reputational concern should be reported rather than pursued through personal confrontation.

The school does not routinely monitor private social-media use. It may consider publicly available material or information lawfully brought to its attention where there is a legitimate safeguarding, conduct, security or reputational concern. Any investigation will be necessary, proportionate and handled under the relevant procedure.

13. ARTIFICIAL INTELLIGENCE AND EMERGING TECHNOLOGY

The school's Artificial Intelligence Policy governs approval and educational use of AI. This policy addresses the associated online-safety risks. AI tools can generate convincing but inaccurate, biased, manipulative or unsafe outputs; imitate people; create or alter images, audio and video; and expose personal or confidential information. Human professional judgement remains essential.

- only approved AI tools may be used for school purposes and use must comply with age restrictions, the AI register, risk assessment and any DPIA or procurement requirements
- personal data, safeguarding records, confidential school information and identifiable pupil work must not be entered into a public or unapproved AI system
- staff must check AI outputs for accuracy, bias, safety, copyright, accessibility and suitability before use
- pupils will be taught to identify AI-generated or manipulated content, verify claims and acknowledge permitted assistance
- AI must not be used for covert surveillance, solely automated high-impact decisions, impersonation, harassment, nudification, sexual content, grooming, discrimination or evasion of school safeguards
- AI-enabled wearable devices are subject to the Mobile Phones and Smart Devices Policy and the AI Policy
- new or materially changed AI tools will trigger review of filtering, monitoring, safeguarding, security and data-protection arrangements.

Any AI-generated nude or semi-nude image of a child, including a deepfake or image created without a real photograph, will be treated under safeguarding procedures and relevant law. The apparent artificial origin of an image does not make the incident harmless.

14. DATA PROTECTION PRIVACY AND RECORDS

Personal data will be processed in accordance with the Data Protection Policy. Online safety does not justify unlimited surveillance or access. Monitoring must be necessary, proportionate, transparent and restricted to legitimate purposes. The school will define who may access monitoring information, how long it is retained, how it is secured and how disclosures are recorded.

- a DPIA will be completed before introducing or significantly changing monitoring or other processing likely to result in high risk to individuals
- privacy information and acceptable-use notices will explain relevant monitoring in clear language
- safeguarding records will be stored in the approved system and access limited to those with a need to know
- monitoring reports supplied to governors will normally be anonymised or aggregated
- personal-data breaches, misdirected communications, loss, unauthorised access or disclosure must be reported immediately through the school's breach procedure
- information may be shared without consent where lawful and necessary to safeguard a child; uncertainty must not delay referral to the DSL.

15. REPORTING AND RESPONDING TO ONLINE SAFETY INCIDENTS

All concerns must be taken seriously. The first priority is the safety and welfare of children and adults, not determining blame or conducting a technical investigation. Staff must use the route below and record facts, actions and decisions.

<u>Concern</u>	<u>Immediate route</u>
A child may be at risk, has disclosed harm, or the incident involves grooming, exploitation, bullying, sexual content, self-harm, extremism or other safeguarding risk	Report immediately to the DSL or deputy DSL and record on the school safeguarding system. If a child is in immediate danger, contact emergency services and then inform the DSL.
An allegation or concern about an adult working with children	Report to the Headteacher under the allegations or low-level-concerns procedure. If the concern is about the Headteacher, report to the Chair of Governors. Do not alert the subject of the concern.
A technical or cyber-security issue without an evident safeguarding element	Stop the activity if safe, disconnect rather than erase where compromise is suspected, and report to technical support and the nominated senior leader.
A personal-data breach	Report immediately to the DPO and follow the Data Protection Policy. The DPO will assess whether notification is required.
Inappropriate pupil behaviour without a safeguarding concern	Report to the relevant teacher or senior leader and manage under the Behaviour and Relationships Policy, while remaining alert to hidden safeguarding needs.

General response principles

- listen calmly, take the child seriously and do not promise confidentiality
- do not ask leading questions or investigate beyond what is necessary to establish immediate safety and reporting
- minimise further exposure; do not forward, download, print, copy or unnecessarily view harmful material
- preserve devices, messages, usernames, URLs, dates and times only in a safe and lawful way; do not delete potential evidence
- consider the needs and safety of the person harmed, witnesses and the child or adult alleged to have caused harm
- inform parents or carers as appropriate, led by the DSL where safeguarding is involved

- consider referrals to children's social care, police, Prevent, the local authority designated officer, CEOP, the Internet Watch Foundation, Report Remove, the platform or other agencies as applicable
- review whether curriculum, supervision, filtering, monitoring, training, risk assessment or policy changes are needed.

16. SAFEGUARDING INCIDENTS AND NUDES AND SEMI NUDES

Online abuse can occur wholly online or facilitate abuse offline. Concerns may include child-on-child abuse, sexual violence or harassment, grooming, exploitation, coercion, cyberbullying, hate, extremist influence, self-harm, suicide, eating-disorder content, trafficking, county lines, financial exploitation or domestic abuse. These concerns must be managed under the Child Protection and Safeguarding Policy.

Where an incident involves the creation, possession or sharing of nudes or semi-nudes, including AI-generated or digitally altered material, staff must follow current UK Council for Internet Safety guidance and the school's safeguarding procedure. A staff member must not view the imagery unless unavoidable, copy it, print it, share it, save it or ask a pupil to send it. The device should be secured only where lawful and necessary, and advice sought from the DSL. The DSL will undertake or oversee the risk assessment and decide on parents, police, children's social care and specialist reporting routes.

The school will avoid language that blames a child for abuse. Support and safety planning will reflect the child's wishes, age, understanding, SEND and wider context. Behaviour consequences may be appropriate but must not replace safeguarding assessment.

17. ILLEGAL CONTENT AND PRESERVING EVIDENCE

If illegal content is suspected - particularly child sexual abuse material, terrorist content, credible threats, serious hate material or content linked to exploitation - staff must stop navigating, avoid further viewing and report immediately to the DSL and Headteacher. They must not search for related material, take screenshots of indecent images, copy files or circulate links.

The DSL or Headteacher will seek advice and make referrals to the appropriate authority. Where a device or system may contain evidence, it should be secured from further use without altering data more than necessary. Technical support may preserve logs or isolate equipment when instructed but must not independently examine suspected indecent imagery. A clear contemporaneous record must identify what was seen, by whom, when, on which device or account, the immediate actions taken and referrals made.

The school will not attempt to determine criminality itself. Police advice will be sought where required. Reporting suspected illegal content in good faith through the school's procedure will be supported.

18. BEHAVIOUR CONSEQUENCES AND STAFF MISCONDUCT

The response to misuse will be proportionate, consistent and based on the seriousness, intent, impact, repetition, age, understanding, SEND, vulnerability, previous incidents and safeguarding context. The school will distinguish an accidental mistake reported promptly from deliberate, harmful or repeated conduct.

<u>Possible response</u>	<u>Examples of when it may be considered</u>
Education and restorative action	Low-level or accidental misuse; misunderstanding; repairing harm where safe and appropriate.
Restriction or removal of access	Unsafe use, attempts to bypass controls, misuse of accounts or devices, or where access creates an immediate risk.
Behaviour sanction	Conduct covered by the Behaviour and Relationships Policy, including cyberbullying, harassment or deliberate misuse.
Safeguarding support or referral	Where a pupil may be at risk, has been harmed, has harmed another child, or behaviour indicates unmet need or exploitation.
Technical or data-protection response	Compromise, malware, unauthorised access, data loss or disclosure.
Staff conduct or disciplinary procedure	Breach of professional boundaries, confidentiality, acceptable use, security or safeguarding duties.
External referral	Where required to police, children's social care, LADO, Prevent, regulators or specialist reporting bodies.

Access restrictions or confiscation will be reviewed and will not prevent a pupil receiving education or support. Staff misconduct concerns must not be handled merely as an online-safety matter where allegations, low-level concerns, disciplinary or whistleblowing procedures apply.

19. MONITORING REVIEW AND GOVERNANCE ASSURANCE

The Online Safety Lead will coordinate an annual review of this policy with the DSL, Headteacher, DPO, Computing Lead, technical support and relevant governors. It will also be reviewed following a serious incident, significant change in guidance, technology or provision, or evidence that arrangements are ineffective.

Assurance will draw on proportionate evidence, including:

- safeguarding and behaviour incident themes
- filtering and monitoring reports, high-risk alerts, checks, exception logs and the recorded annual review
- technical-security incidents, access reviews and data breaches
- pupil, staff and parent voice
- curriculum coverage and assessment
- training and induction records
- complaints and lessons learned
- changes in devices, services, AI use and the school's risk profile.

Governors will receive an annual report and timely notification of serious issues as appropriate. Reports will protect confidentiality and contain enough information to support challenge, assurance and improvement. Actions will identify an owner and timescale and will be tracked to completion.

20. APPENDIX A - IMMEDIATE RESPONSE GUIDE

<u>Step</u>	<u>Action</u>
1 Make safe	Address immediate danger; stop or minimise exposure; reassure the child; call emergency services where required.
2 Report	Safeguarding concern to DSL or deputy immediately; adult concern to Headteacher or Chair; data breach to DPO; technical issue to technical support and SLT.
3 Do not investigate	Do not search, forward, copy, print or save suspected illegal or indecent content. Do not ask leading questions.
4 Preserve appropriately	Record facts, time, account, device and URL if safe. Secure the device without unnecessary manipulation. Preserve logs through authorised technical support.
5 Assess and refer	DSL or relevant lead assesses risk and contacts parents, police, children's social care, LADO, Prevent or specialist services as appropriate.
6 Support and record	Support all affected children; record decisions, actions and outcomes in the correct system.
7 Learn	Review supervision, teaching, filtering, monitoring, security, privacy, training and policy implications.

If in doubt, treat the matter as a safeguarding concern and contact the DSL. Do not allow uncertainty about the technology to delay action for a child.

21. APPENDIX B - FILTERING AND MONITORING REVIEW RECORD

This appendix provides the minimum record for the annual review. The completed review should be retained with supporting evidence and reported to governors.

<u>Review field</u>	<u>Record</u>
Date and trigger	Annual review or reason for additional review
People involved	Senior leader, DSL, technical support, responsible governor, DPO or others
Current provision	Provider, networks, devices, off-site coverage, user groups, monitoring methods and report routes
Risk profile	Age, SEND, EAL, vulnerabilities, curriculum, remote use, BYOD, AI and local or contextual risks
Filtering checks	Illegal-content categories, adult content, profiles, images, multilingual content, backup connections, guest access and off-site devices
Monitoring checks	Weekly report, immediate high-risk alerts, identifiable users, manual supervision, access and escalation
Privacy and security	Transparency, authorised access, retention, security, contracts and DPIA status
Incidents and trends	Relevant safeguarding, behaviour, cyber and data-protection evidence
Teaching impact	Overblocking, underblocking, curriculum requirements and exception decisions
Findings and actions	Gap, risk rating, action, owner, deadline and completion evidence
Approval and assurance	DSL, senior leader, technical support and governor sign-off or meeting record