BURTON HATHOW
PREPARATORY SCHOOL

| | |
|---|---|
| **Policy owner** | **Headteacher / Designated Safeguarding Lead** |
| **Last updated** | August 2026 |
| **Effective from** | 1 September 2026 |
| **Review cycle** | At least annually and after significant change or incident |
| **Next scheduled review** | August 2027 |

# Contents

Statement of intent

1. Legal and regulatory framework
2. Roles and responsibilities
3. Whole-school approach to online safety
4. Cyberbullying
5. Child-on-child abuse, harassment and violence (including online)
6. Grooming, exploitation and radicalisation
7. Mental health, wellbeing and online harms
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Staff training and awareness
11. Online safety and the curriculum
12. Use and procurement of technology in the classroom
13. Mobile phones, smart technology and wearables
14. Working with parents and carers
15. Internet and network access
16. Filtering and monitoring
17. Cyber security and network security
18. Email and electronic communications
19. Generative artificial intelligence (AI)
20. Social networking and professional boundaries
21. School website and digital publishing
22. School-owned and BYOD devices
23. Remote education
24. Data protection, privacy and EdTech
25. Digital leadership, governance and technology strategy
26. Incident response, reporting and evidence
27. Monitoring and review

Appendix A: The 4Cs risk framework

Appendix B: Minimum filtering and monitoring assurance checks

Appendix C: Key statutory and DfE references

## Statement of intent

Burton Hathow Preparatory School recognises that technology is integral to education, communication and modern life. The school is committed to enabling pupils to benefit from digital technology while protecting them from harm and helping them develop the knowledge, judgement and resilience to use technology safely, respectfully and lawfully.

Online safety is a safeguarding responsibility. It is not treated as a stand-alone technical issue: it is a running and interrelated theme within safeguarding, behaviour, curriculum, staff conduct, data protection, digital strategy, procurement and parental engagement.

In accordance with Keeping Children Safe in Education (KCSIE) 2026, the school uses the four areas of online risk — content, contact, conduct and commerce — as the basis of its approach. The school recognises that risks are continually evolving, including risks arising from generative AI, AI-generated or manipulated imagery, personalised and dynamic content, online sexual abuse, scams, misinformation and harmful interaction with automated or simulated systems.

This policy applies to all pupils, staff, volunteers, governors/proprietors, contractors and visitors using the school's digital technology, networks or services, and to online behaviour outside school where it affects the safety or welfare of pupils or the school community.

## 1. Legal and regulatory framework

This policy has due regard to current legislation, statutory guidance and national standards applicable in England, including:

- Keeping Children Safe in Education 2026 (DfE), effective from 1 September 2026.
- Education (Independent School Standards) Regulations 2014, including safeguarding and welfare requirements.
- Working Together to Safeguard Children (statutory guidance), as updated.
- Early Years Foundation Stage statutory framework, where applicable to school-based early years provision.
- Prevent Duty Guidance: England and Wales (2023), as amended.
- Mobile phones in schools: statutory guidance (DfE, 2026), to be followed from 1 September 2026.
- DfE Meeting digital and technology standards in schools and colleges, including the filtering and monitoring, cyber security and digital leadership and governance core standards (updated 25 August 2026).
- DfE Teaching online safety in schools guidance.
- DfE Harmful online challenges and online hoaxes guidance.
- DfE Searching, screening and confiscation guidance, where relevant.
- DfE Generative artificial intelligence (AI) in education guidance and Generative AI: product safety standards (updated January 2026).
- UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- UKCIS Education for a Connected World framework.
- Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025.
- ICO Children's Code (Age Appropriate Design Code) and relevant ICO guidance.
- Computer Misuse Act 1990.
- Copyright, Designs and Patents Act 1988.
- Voyeurism (Offences) Act 2019 and other relevant criminal law.
- National Cyber Security Centre (NCSC) guidance and Cyber Essentials-aligned good practice.

This policy should be read alongside the school's current:

- Child Protection and Safeguarding Policy
- Behaviour and Anti-Bullying Policies
- Child-on-child Abuse / Harmful Sexual Behaviour procedures
- Staff Code of Conduct and allegations/low-level concerns procedures
- Acceptable Use Agreements for staff and pupils
- Social Media Policy
- Data Protection Policy, privacy notices and DPIA register
- Cyber Security / Cyber Response and Recovery arrangements
- Photography, Images and Video Policy
- Device / BYOD User Agreement
- Prevent Duty Policy and Prevent risk assessment
- Remote Education Policy
- School Website Policy
- Business continuity and disaster recovery arrangements

## 2. Roles and responsibilities

### Board / Proprietor

- Has overall strategic responsibility for safeguarding, including online safety and filtering and monitoring.
- Ensures appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least once every academic year.
- Identifies a governor/proprietor link for filtering and monitoring and, where practicable, digital technology.
- Receives sufficient assurance about filtering and monitoring, cyber security, significant incidents, identified gaps and resulting actions.
- Ensures the school is working towards the DfE's six core digital and technology standards by 2030, while recognising that the filtering and monitoring core standard should already be met.
- Supports and challenges the school's digital strategy, cyber risk management and major technology procurement decisions.

### Headteacher / responsible SLT member

- Ensures online safety is embedded throughout safeguarding, policy, curriculum, training, behaviour and parental engagement.
- Ensures a member of SLT is explicitly responsible for filtering and monitoring and a member of SLT is responsible for digital technology. These responsibilities may be held by the same person.
- Coordinates the annual filtering and monitoring review with the DSL, IT support and responsible board member/proprietor, and ensures a written record and action plan are retained.
- Ensures filtering and monitoring checks are completed and recorded at a frequency informed by the school's risk assessment.
- Ensures the school maintains and reviews a cyber risk assessment annually and revisits it at least termly, in line with the DfE cyber security core standard.
- Ensures staff are trained in their online safety, filtering/monitoring, cyber security and reporting responsibilities.
- Ensures new technology, significant configuration changes, BYOD changes and learner-facing AI tools are risk-assessed before implementation.

## Designated Safeguarding Lead (DSL)

- Takes lead responsibility for safeguarding and online safety.
- Understands the unique risks associated with online safety and the additional risks that children with SEND may face online.
- Works with the responsible SLT member and IT support to review filtering and monitoring arrangements and identify safeguarding risks.
- Checks relevant monitoring reports and alerts, ensures concerns are acted on promptly, and escalates or refers safeguarding concerns in line with KCSIE and local procedures.
- Ensures staff know how to report online safety concerns, including concerns arising from monitoring alerts, AI-generated content, harmful sexual behaviour and image-sharing.
- Maintains accurate safeguarding records and considers patterns, trends and groups of pupils who may be more vulnerable.
- Ensures pupils' views, wishes and experiences inform safeguarding responses where appropriate.

## IT support / (Blue Cube)

- Maintains the school's technical filtering, monitoring, cyber security and network controls.
- Provides reports and technical assurance to SLT and the DSL, completes actions arising from checks and incidents, and supports the annual review.
- Ensures relevant illegal-content blocklists, including IWF and CTIRU lists where supplied through the filtering service, are implemented and protected from unauthorised override.
- Ensures filtering profiles are appropriately differentiated for pupils, staff and guests and that system changes are documented.
- Tests filtering and monitoring after material changes, updates and deployment of new school-managed devices or services.
- Maintains appropriate patching, anti-malware, firewall, authentication, backup and logging arrangements in line with the DfE cyber security standards.

## All staff

- Take responsibility for safe and secure use of the systems and data they access.
- Understand that safeguarding includes online harm and maintain an attitude that 'it could happen here'.
- Know how the school's filtering and monitoring arrangements affect their role, how to report concerns and what to do if inappropriate content is accessed.
- Use school-approved technology and accounts for school business and comply with the Staff Code of Conduct and Acceptable Use Agreement.
- Model safe, respectful and lawful digital behaviour and embed online safety into teaching where relevant.
- Report safeguarding concerns to the DSL immediately and technical/security concerns through the school's IT reporting route.

## Pupils

- Follow the pupil Acceptable Use Agreement, Behaviour Policy and device/BYOD rules.
- Use school technology for appropriate educational purposes and respect the privacy and rights of others.
- Tell a trusted adult if they see, receive or are asked to create or share anything that worries, frightens or pressures them.
- Do not attempt to bypass filtering, use unauthorised mobile data or hotspots, install unauthorised software, access another person's account or interfere with school systems.

## 3. Whole-school approach to online safety

The school uses a child-centred, whole-school approach. Online safety is addressed through safeguarding systems, curriculum teaching, supervision, technical controls, behaviour expectations, staff conduct, parent engagement and prompt response to concerns.

- Online safety concerns are treated first and foremost as safeguarding concerns where there is a risk of harm.
- Staff do not promise confidentiality where information must be shared to keep a child or another person safe.
- Pupils who display harmful online behaviour may themselves be vulnerable or have been harmed; responses consider the needs of all children involved.
- Concerns about staff or volunteers are reported to the Headteacher; concerns about the Headteacher are reported to the Chair/Proprietor, in line with KCSIE and school procedures.
- Potentially criminal behaviour is referred to the police and/or other appropriate agencies. Illegal child sexual abuse imagery should be reported through the appropriate safeguarding and law-enforcement routes; staff must not intentionally view, copy, print or forward such material.
- Where an online incident occurs outside school but affects pupils' safety, relationships or education, the school may act under safeguarding and behaviour procedures.

## 4. Cyberbullying

Cyberbullying includes repeated or serious online behaviour intended to threaten, humiliate, exclude or harm another person. It may include abusive messages, impersonation, sharing images, doxxing, discriminatory abuse, sexualised bullying, group-chat exclusion, coercion or the use of AI-generated or manipulated content.

Cyberbullying is managed under the Behaviour, Anti-Bullying and Safeguarding Policies. The school will avoid language that trivialises harmful behaviour and will consider whether the conduct constitutes child-on-child abuse or a criminal offence.

## 5. Child-on-child abuse, harassment and violence (including online)

Child-on-child abuse can occur inside or outside school and online or offline. It may include bullying, abuse in intimate personal relationships, physical abuse, sexual violence and harassment, upskirting, initiation/hazing behaviours, coercion, stalking, image-based abuse and the making or sharing of nudes or semi-nudes.

For the purposes of this policy, nudes and semi-nudes include visual content created, taken, altered or wholly generated by artificial intelligence, including deepfakes or 'deep nudes'. Staff must report such concerns immediately to the DSL and follow the school's safeguarding response; they must not ask pupils to forward images or search devices themselves unless acting under an authorised school procedure.

The school adopts a zero-tolerance approach to sexual harassment and sexual violence in the sense that it is never accepted, normalised or dismissed as 'banter', while ensuring responses are proportionate, child-centred and consistent with KCSIE.

## 6. Grooming, exploitation and radicalisation

- Staff are alert to online grooming indicators such as secrecy, coercive relationships, unexplained gifts or devices, pressure to move conversations to private channels, requests for imagery, threats, blackmail or financial demands.

- Child sexual exploitation (CSE) and child criminal exploitation (CCE) can be facilitated or organised online. Concerns are reported to the DSL without delay.
- Online financial exploitation, including sextortion and fraud, is recognised as a safeguarding risk.
- The school's Prevent risk assessment informs online safety, curriculum, filtering and monitoring decisions. Radicalisation concerns are managed through the DSL and the Prevent Duty procedures.

## 7. Mental health, wellbeing and online harms

Staff recognise that online experiences can affect mental health and wellbeing, including through bullying, harassment, extreme or self-harm content, unrealistic comparison, compulsive use, sexualised content, manipulative design, AI companionship or simulated relationships.

Concerns about a child's wellbeing are responded to through pastoral and safeguarding systems. Where there is an immediate risk of harm, the school follows its safeguarding and emergency procedures.

## 8. Online hoaxes and harmful online challenges

The DSL assesses reports case by case, considering credibility, scale, age and developmental stage, vulnerability and the risk of amplification. Communications are proportionate, factual and based on reliable sources. The school avoids unnecessarily naming or describing harmful challenges in ways that could increase curiosity or participation.

## 9. Cyber-crime

Pupils are taught that cyber-enabled and cyber-dependent offending can cause serious harm and may be criminal. This includes unauthorised access, password attacks, malware, denial-of-service activity, account compromise, data theft and deliberate interference with networks or devices.

Where appropriate, the school may seek advice from police or the National Crime Agency's Cyber Choices programme to divert a child from cyber offending while addressing any underlying safeguarding needs.

## 10. Staff training and awareness

- All staff receive safeguarding and child protection training at induction, including online safety and their responsibilities in relation to filtering and monitoring.
- All staff receive regular safeguarding updates, including online safety, as required and at least annually.
- Staff who manage filtering, monitoring, digital technology or cyber security receive role-appropriate training and information from the school and/or provider.
- Training includes emerging risks such as AI-generated content, deepfakes, online sexual abuse, scams, phishing, harmful content, cyber incidents and appropriate use of school systems.
- Records of training, briefings and attendance are retained.

## 11. Online safety and the curriculum

Online safety is embedded across the curriculum, including Relationships Education, Health Education, PSHE and Computing. Teaching is age-appropriate, developmentally appropriate and adapted where needed for pupils with SEND or other vulnerabilities.

- How people may behave differently online or pretend to be someone else.
- How to recognise harmful content, contact and behaviour and how to report it.
- Privacy, personal information, passwords, consent and the implications of sharing data and images.
- Online reputation, respectful communication, bullying and bystander behaviour.

- Critical evaluation of information, misinformation, disinformation, fake news, persuasion and AI-generated content.
- Scams, phishing, financial exploitation, in-app purchases and gambling-related risks.
- Copyright, intellectual property, academic integrity and responsible use of generative AI.
- Healthy use of technology and routes to support.

External visitors or resources used for online safety education are checked for suitability. Staff remain present and responsible for the safeguarding and educational context of any external session.

## 12. Use and procurement of technology in the classroom

- Staff use school-approved platforms, apps and services for teaching. Examples may include Showbie, Bug Club and approved programming or productivity tools.
- New digital products are considered for educational value, safeguarding, accessibility, data protection, age appropriateness, information security, compatibility, ongoing support and cost before adoption.
- Where a product processes personal data, the school follows its data protection procurement process and completes a DPIA where the processing is likely to result in high risk or where otherwise advised by the DPO.
- Teachers pre-check unfamiliar resources and understand that filtering cannot guarantee that all dynamic, personalised or AI-generated content will be safe.
- Any change to filtering for curriculum purposes must be authorised, documented, proportionate and time-limited. Illegal-content blocklists must never be disabled or overridden.

## 13. Mobile phones, smart technology and wearables

From 1 September 2026, the school follows the DfE statutory guidance that schools should be mobile phone-free environments by default. Pupils must not have access to or use mobile phones throughout the school day, including lessons, movement between lessons, breaks and lunchtime, except where a documented exception applies.

- The restriction also applies to smart technology with similar communication or recording functionality where the school has included it within its rules, such as connected smartwatches.
- Reasonable adjustments or exceptions may be made for medical, disability or SEND needs, or another exceptional circumstance, following an individual assessment.
- Where pupils bring a phone for travel or safeguarding reasons, it must be handed in or stored using the school's agreed secure method and must remain inaccessible during the school day.
- Personal hotspots, tethering and mobile-data connections must not be used by pupils to bypass the school network, filtering or monitoring.
- Staff use of personal devices is governed by the Staff Code of Conduct.

## 14. Working with parents and carers

- The school communicates its online safety, mobile phone and device expectations clearly to parents and carers.
- Parents are informed, in accessible terms, that filtering and monitoring systems are used and that no system is completely effective.
- Remote-learning communications identify the platforms pupils will use and who from school they may interact with online.
- The school signposts trusted sources of advice such as CEOP, UK Safer Internet Centre, Internet Matters and relevant DfE/NCSC resources.

- Parents are encouraged to discuss age-appropriate technology use, privacy settings, parental controls, reporting routes and the risks of mobile data bypassing school controls.

## 15. Internet and network access

- Users access school digital services only through authorised accounts and in accordance with the relevant Acceptable Use Agreement.
- School network access is segmented and controlled appropriately for pupils, staff, guests and devices.
- Pupil learning devices used on site must use the school's authorised network unless a specific exception has been approved. Mobile data, tethering or personal hotspots must not be used to bypass school controls.
- Guest access is provided only where appropriate and is subject to suitable filtering and security controls.
- Attempts to bypass filtering, monitoring, authentication or network controls are treated as a safeguarding and/or disciplinary concern.

## 16. Filtering and monitoring

The school will meet the DfE Filtering and Monitoring Core Standard. Filtering is preventative and is used to restrict access to illegal, inappropriate and potentially harmful content. Monitoring is reactive and is used to identify concerning activity, patterns or alerts so that safeguarding action can be taken.

### Governance and review

- The Board/Proprietor has overall strategic responsibility. A responsible SLT member, responsible board member/proprietor, DSL and IT support work together to provide assurance.
- A formal review of filtering and monitoring provision is completed at least once every academic year and additionally when safeguarding risk changes, BYOD/remote working changes, new technology or AI tools are introduced, major software updates occur, or network/device configuration changes materially.
- The review records current provision, gaps, risk profile, technical limitations, relevant incidents, BYOD use, generative AI use, monitoring strategy, staff training and actions.
- The school keeps a written record of the review and actions taken, available for inspection by those entitled to see it.

### School arrangements

- Filtering and monitoring are provided through Securly and managed with the school's IT service provider, Blue Cube, subject to regular school oversight.
- The school uses differentiated filtering profiles appropriate to user groups; it does not rely on one blanket profile for all users.
- IWF and CTIRU illegal-content blocklists are implemented through the filtering solution and must not be disabled, overridden or altered by school users or administrators.
- The school considers whether its provision can address real-time, dynamic, personalised and AI-generated content, and records any limitations and mitigations.
- Monitoring reports and alerts that may indicate a safeguarding concern are reviewed through an agreed triage process involving the DSL or safeguarding team.

### Checks and records

- Filtering and monitoring checks are risk-based. The school currently expects operational checks at least monthly, with additional checks following significant changes or concerns.

- Checks cover school-managed internet-connected devices and services, relevant locations, and user profiles for pupils, staff and guests.
- The school records the date, person carrying out the check, what was tested, the outcome and any actions.
- New school-managed devices and services are checked before deployment to confirm that filtering and monitoring work as intended.
- At minimum, filtering checks include assurance that illegal child sexual abuse material, unlawful terrorist content and adult content are blocked, using provider assurance and/or appropriate testing tools.

### Proportionality and privacy

Filtering must not unreasonably restrict teaching and learning. Monitoring is carried out only for legitimate safeguarding, security and operational purposes and in accordance with privacy notices, data protection law and the school's monitoring arrangements.

## 17. Cyber security and network security

The school works towards and applies the DfE Cyber Security Core Standard as part of its digital strategy and safeguarding arrangements.

- A cyber risk assessment is completed annually and revisited at least termly, and after a significant incident or technology/process change.
- Cyber risks are recorded, prioritised and linked to business continuity, disaster recovery and the school's cyber response plan.
- Digital assets, software, cloud services and data-processing systems are recorded in appropriate registers and are supported, licensed and updated.
- Security updates and patches are applied promptly according to risk and provider guidance.
- Firewalls and anti-malware protections are maintained. Unauthorised software and browser extensions must not be installed.
- Multi-factor authentication is used for accounts with access to sensitive personal or operational data where supported/required, and privileged/admin access is tightly controlled.
- Users have unique accounts and receive only the access needed for their role. Shared accounts are avoided except where technically necessary and risk-managed.
- Passwords and authentication credentials must not be shared. Devices must be locked when unattended.
- Backups are maintained, protected from routine user access and periodically tested for restoration.
- Network and system logging is maintained at a level proportionate to the school's risks and technical environment.
- Cyber incidents are reported immediately through the school's cyber response process and, where appropriate, to the DPO, insurers, NCSC, ICO, police or other relevant bodies.

## 18. Email and electronic communications

- Staff use school-issued accounts for school business. Personal email accounts must not be used to conduct school business unless expressly authorised in an emergency and then regularised promptly.
- Sensitive or personal information is shared using approved secure methods appropriate to the risk. Encryption or secure portals are used where required by the school's data protection procedures.
- Staff remain alert to phishing, impersonation, fraudulent payment requests and malicious attachments or links and report suspicious communications promptly.

- Email security settings, including controls intended to reduce spoofing and impersonation, are maintained by IT support.
- Phishing and cyber-awareness training is provided regularly; simulated exercises may be used proportionately.

## 19. Generative artificial intelligence (AI)

The school recognises that generative AI can support education and administration but can also create safeguarding, privacy, intellectual-property, misinformation, bias, manipulation, assessment and developmental risks. Use is therefore subject to school approval, age-appropriate controls and risk assessment.

### Learner-facing AI

- Learner-facing generative AI must be specifically approved before use and must be appropriate for the pupils' age, developmental stage and needs.
- The school will consider DfE Generative AI Product Safety Standards, including filtering, security, privacy, transparency, governance, child-centred design, cognitive development, mental health and manipulation risks.
- The school considers whether AI interactions simulate human relationships or create harmful contact risks, and whether generated text, images, audio or video can bypass existing filters.
- Pupils must not use generative AI to create sexualised, abusive, deceptive or harmful material, impersonate another person, generate deepfakes, evade safeguarding controls or facilitate bullying.

### Staff use

- Staff remain professionally responsible for the accuracy, suitability, bias and safeguarding implications of material produced with AI.
- AI output must not be treated as authoritative without appropriate checking, particularly for safeguarding, legal, medical, assessment or other high-stakes decisions.
- Identifiable pupil, parent or staff data, safeguarding information, special-category data or confidential school information must not be entered into public or unapproved AI tools.
- Where an approved AI system processes personal data, the school establishes a lawful basis, data-processing terms, security controls, retention arrangements and a DPIA where required.
- Staff must respect copyright and intellectual-property rights and must not upload protected material to AI systems for training or commercial reuse without a lawful basis or permission.
- Use of AI in assessment must comply with school assessment rules and any relevant awarding-body requirements.

## 20. Social networking and professional boundaries

Staff and pupil use of social media is governed by this policy Staff Code of Conduct and Behaviour Policy. Staff maintain professional boundaries, appropriate privacy settings and do not communicate with pupils through personal social media accounts except where a formally approved school system or safeguarding arrangement applies.

Online conduct that may raise a safeguarding or suitability concern is managed under KCSIE, the Staff Code of Conduct, allegations procedures and low-level concerns procedures as appropriate.

## 21. School website and digital publishing

- The Headteacher ensures website and digital-publication content is appropriate, accurate and compliant with statutory information requirements.
- Personal data, photographs and video are published in accordance with the school's privacy notices, data protection procedures.
- Staff consider safeguarding, location, identification and contextual risks before publishing content about pupils or school activities.
- School-controlled social media and website accounts use appropriate access controls and are reviewed when staff responsibilities change.

## 22. School-owned and BYOD devices

### School-owned devices

- School-owned devices are configured, maintained and monitored in accordance with this policy and the Device User Agreement.
- Filtering and monitoring must be confirmed as operational before new school-managed devices are distributed.
- School-managed devices remain subject to school security and monitoring controls when taken off site where the technical solution provides this.

### Bring Your Own Device (BYOD)

- BYOD is permitted only under the school's BYOD/Device User Agreement and only for approved educational purposes.
- On site, pupil BYOD learning devices must connect through the school's authorised filtered network. Cellular/mobile data, personal hotspots and tethering must be disabled and must not be used to bypass school controls.
- BYOD arrangements are included explicitly in the annual filtering and monitoring review and are reviewed whenever the scheme changes.
- The school may require specified security settings, operating-system versions, passcodes or management profiles as a condition of BYOD access.
- The school cannot guarantee the safety or security of content accessed away from the school network on a privately owned device; parents remain responsible for appropriate home controls and supervision.

## 23. Remote education

- Remote education uses school-approved platforms and follows KCSIE and DfE safeguarding guidance.
- Parents and pupils are told which sites and platforms will be used and who from school the pupil may interact with online.
- Staff follow professional-boundary and recording expectations when communicating remotely with pupils.
- Where school-managed devices are used remotely, school security, filtering and monitoring controls apply where technically supported.
- Safeguarding concerns arising during remote learning are reported through the same school safeguarding procedures as concerns arising on site.

## 24. Data protection, privacy and EdTech

The school complies with the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025. The 2025 Act amends and builds on the existing data protection framework; it does not replace UK GDPR or the Data Protection Act.

- Personal data is processed lawfully, fairly, transparently and securely, and only for defined purposes.
- Access to pupil, staff and parent data is limited according to role and need.
- New EdTech procurement considers data protection, safeguarding, security, accessibility, supplier terms, data location/processing, retention, sub-processors and exit arrangements.
- A DPIA is completed where processing is likely to result in high risk to individuals and where advised by the DPO.
- Privacy information explains significant monitoring or data processing in clear and accessible terms.
- The school maintains a clear process for handling data protection concerns and complaints.

## 25. Digital leadership, governance and technology strategy

The school will work towards the DfE's six core digital and technology standards by 2030: broadband internet, wireless network, network switching, digital leadership and governance, filtering and monitoring, and cyber security. The school recognises that the filtering and monitoring core standard should already be met.

- The Headteacher assigns an SLT digital technology lead with strategic oversight of digital technology and its alignment with the School Development Plan.
- The school maintains up-to-date registers for relevant hardware, systems, licences/subscriptions, approved apps/services and information assets.
- Digital technology is included within business continuity and disaster recovery planning.
- The school maintains a digital technology strategy of at least two years, reviewed at least annually and informed by curriculum, safeguarding, SEND/accessibility, data protection, cyber risk, budget and sustainability considerations.
- The Board/Proprietor supports and challenges the digital technology strategy and major risk or investment decisions.
- The school uses the DfE 'Plan technology for your school' service as a self-assessment and improvement tool where appropriate.

## 26. Incident response, reporting and evidence

- Safeguarding concerns are reported to the DSL through the school's established safeguarding system without delay.
- Urgent concerns about a child's immediate safety are escalated immediately and emergency services are contacted where necessary.
- Technical incidents, malware, suspected account compromise, data loss or unauthorised access are reported promptly to IT support and the responsible SLT member.
- Where a personal data breach may have occurred, the DPO is informed promptly so that notification obligations can be assessed.
- Staff preserve relevant evidence without unnecessarily viewing, copying or redistributing harmful or illegal material.
- Incident records include what happened, actions taken, referrals made or not made, and the rationale for decisions.

## 27. Monitoring and review

This policy is reviewed at least annually by the Headteacher, DSL and Board/Proprietor and sooner where there is a significant safeguarding incident, change in law or statutory guidance, material change in technology or working practice, or significant change to filtering/monitoring, BYOD or AI use.

Operational practice, filtering/monitoring checks, cyber risk, training needs and actions arising from incidents are reviewed more frequently in accordance with the risk assessments and standards described above.

Next scheduled policy review: August 2027.

## Appendix A: The 4Cs risk framework

| Risk | Examples | School response |
|---|---|---|
| Content | Pornography; racism; misogyny; antisemitism; self-harm/suicide; radicalisation/extremism; extreme sexual or physical violence; misinformation/disinformation; conspiracy theories; harmful AI-generated material. | Age-appropriate teaching; filtering; supervision; reporting routes; targeted support. |
| Contact | Harmful interaction with other users or generative AI systems that simulate interaction; grooming; pressure; exploitation; commercial contact; sextortion. | Trusted-adult reporting; safeguarding response; platform controls; monitoring; CEOP/police/CSC referral where appropriate. |
| Conduct | Bullying; harassment; making/sending/receiving explicit images, including AI-generated images; impersonation; deepfakes; privacy breaches; harmful posting. | Behaviour and safeguarding procedures; education; restorative/supportive work where appropriate; sanctions/referral where necessary. |
| Commerce | Gambling; scams; phishing; fraudulent offers; inappropriate advertising; in-app purchases; financial exploitation. | Filtering; cyber education; parent guidance; incident reporting; financial/cyber-security controls. |

## Appendix B: Minimum filtering and monitoring assurance checks

☐ Responsible SLT member, DSL, responsible governor/proprietor and IT support roles are current and documented.
☐ Annual formal review completed and actions tracked.
☐ Monthly/risk-based operational check log is current.
☐ Filtering active on all school-managed internet-connected devices and relevant services.
☐ Correct pupil, staff and guest profiles are applied.
☐ IWF and CTIRU blocklists are confirmed through provider assurance/configuration.
☐ Adult content, illegal child sexual abuse material and unlawful terrorist content are blocked.
☐ Monitoring alerts and reports are reaching the agreed recipients and safeguarding triage is functioning.
☐ BYOD arrangements, mobile data/hotspot risks and remote-device use have been considered.

☐ Generative AI products and AI-generated/dynamic content limitations have been considered.
☐ Temporary filtering exceptions are authorised, recorded and time-limited.
☐ New devices/services and major configuration changes are tested before use.
☐ Staff know how to report filtering failures, concerning searches/content and monitoring alerts.

## Appendix C: Key statutory and DfE references

The policy should be checked against the live versions of the following sources at each formal review:

- Department for Education — Keeping Children Safe in Education 2026.
- Department for Education — Meeting digital and technology standards in schools and colleges (updated 25 August 2026).
- Department for Education — Filtering and monitoring: core standard.
- Department for Education — Cyber security: core standard.
- Department for Education — Digital leadership and governance: core standard.
- Department for Education — Mobile phones in schools (statutory guidance, 2026).
- Department for Education — Generative artificial intelligence (AI) in education.
- Department for Education — Generative AI: product safety standards (updated 19 January 2026).
- Department for Education — Data protection in schools, including Data (Use and Access) Act 2025 updates.
- UKCIS — Sharing nudes and semi-nudes guidance and Education for a Connected World.
- NCSC — current cyber-security guidance for schools and organisations.