EMBARK FEDERATION

Love Learning, Love Life.

Our school is part of the Embark Federation.

The shared vision for our trust is to “create schools that ‘stand out’ at the heart of their communities.” Our trust has four core beliefs; Family, Integrity, Teamwork and Success that are integral to everything we do. The purpose is to enable everyone to be able to ‘Love Learning, Love Life.’

Our policies are underpinned by our vision, beliefs and purpose.

Online Safety Policy and Procedures

Date of Issue	01/09/2026
Date of Review	01/09/2027
Version	V7
Approval Level	CEO

Change history
Legal framework refreshed; roles and responsibilities aligned to KCSIE 2024; sexting section updated with DDSCP procedures and NCMEC Take It Down; communications table amended; audit tools added; generative AI content introduced; Network Manager retitled IT Lead; signatory updated to David King.

Full redraft for the 2026/27 academic year. Substantive changes:

- Aligned throughout to Keeping Children Safe in Education 2026 (in force 1 September 2026), including the updated 4Cs risk categories, the term "nudes and semi-nudes", and the requirement that the effectiveness of filtering and monitoring is reviewed at least once every academic year with named accountability and retained evidence.
- New Section 10: Mobile phones and personal devices, reflecting the DfE's Mobile phones in schools guidance (updated January 2026) and section 36 of the Children's Wellbeing and Schools Act 2026, which gives that guidance the force of law from 29 June 2026. The previous communications table, which allowed student phone use at social times, has been superseded.
- New Section 7: Cyber security and digital resilience — multi-factor authentication, patching, backups, supplier assurance, incident response and reporting routes.
- Section 9 (Generative AI) substantially expanded: approved tools register, DPIA before deployment, AI chatbots and companion apps as a contact risk, AI-generated and digitally altered imagery, academic integrity, and the June 2026 changes to the DfE Filtering and Monitoring Standards on AI-generated content.
- Section 12 rewritten as "Nudes and semi-nudes", covering AI-generated and digitally altered images, and confirming that all incidents require a safeguarding response whether consensual or non-consensual. Report Remove added alongside Take It Down.
- New Section 13: additional online harms — sextortion, harmful online challenges and hoaxes, self-harm and suicide content, misogyny and harmful sexual behaviour, gambling and financial harm, online criminal exploitation, and misinformation.
- New content on remote learning and online meetings, vulnerable students, student voice, visitors and external providers, and parents' own online conduct.
- Password guidance aligned to NCSC advice (length and uniqueness over routine expiry; MFA on privileged accounts).
- Duplication between the former sections 4, 13 and 15 removed; "Network Manager" replaced with "IT Lead" throughout; numbering, citations and broken links corrected.
- New Appendix 4 (online safety incident log template) and Appendix 5 (AI tool approval checklist).
- Final KCSIE 2026 alignment review: expanded the 4Cs Content examples to mirror KCSIE more closely, including racism, misogyny, antisemitism, radicalisation, extremism and extreme sexual or physical violence.
- Clarified filtering and monitoring accountability so that the named SLT lead with strategic responsibility leads the annual effectiveness review, supported by the DSL, IT Lead and trust IT service.
- Added an explicit link between this policy and the Child Protection and Safeguarding Policy, including the requirement that filtering and monitoring arrangements are reflected there.
- Clarified governance arrangements for a trust-wide policy: central approval in accordance with the Scheme of Delegation, with local governing teams responsible for local assurance and effective implementation.

Contents

1. Introduction, scope and areas of risk

Our school understands that using online services and a range of devices, both in school and for remote learning, is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning.

Using online services and devices safely brings significant benefits in equipping children to navigate a rapidly advancing world. A number of controls need to be in place to ensure the safety of students and staff.

Scope

This policy applies to all members of the school community — staff, students, volunteers, governors and trustees, parents and carers, visitors, contractors, external providers and community users — who have access to, or are users of, school ICT systems, whether on or off the school site.

It applies to the use of school devices and systems anywhere, and to the use of personal devices where the conduct in question affects, or is likely to affect, the safety or wellbeing of a member of the school community, or the reputation of the school. The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site.

The four areas of risk

Keeping Children Safe in Education categorises online risk under four headings. These categories were updated in the 2026 edition to reflect the growing presence of artificial intelligence, and our curriculum, filtering, monitoring and risk assessment are all mapped against them:

- Content: being exposed to illegal, inappropriate or harmful material — for example pornography, racism, misogyny, antisemitism, radicalisation and extremism, extreme sexual or physical violence, self-harm and suicide content, pro-eating-disorder material, and misinformation, disinformation and conspiracy theories. This includes content generated by AI.
- **Contact:** being subjected to harmful online interaction — for example peer pressure, commercial advertising, adults posing as children in order to groom or exploit, and harmful interactions with generative AI applications that simulate human interaction, such as chatbots and companion-style systems.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm — for example making, sending or receiving explicit images (including images generated or altered using AI), online bullying, and the sharing of others' personal information.
- **Commerce:** risks such as online gambling and loot boxes, inappropriate advertising, phishing, sextortion and other financial scams.

The measures set out in this policy revolve around these four areas of risk.

Other risks the school seeks to manage

- Unauthorised access to, loss of, or sharing of personal information
- The risk of being groomed by those with whom students make contact online
- The sharing or distribution of personal images without consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Online bullying and online hate
- Access to unsuitable video content, games or livestreams
- Online criminal and sexual exploitation, including recruitment through social media and gaming platforms

- The impact of excessive or compulsive use on sleep, wellbeing, social and emotional development and learning
- Cyber attacks against the school or trust that disrupt learning or compromise personal data

Many of these risks reflect situations in the offline world, and it is essential that this policy is used in conjunction with other school policies, including the Child Protection and Safeguarding Policy, the Behaviour Policy and the Anti-Bullying Policy. The key principles and arrangements in this Online Safety Policy, including the Trust's approach to filtering and monitoring, are reflected within the Child Protection and Safeguarding Policy in accordance with Keeping Children Safe in Education.

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

2. Legal framework and related guidance

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following. Where a document is updated, the current version applies.

Legislation

- Children Act 1989 and Children Act 2004
- Protection of Children Act 1978 and Criminal Justice Act 1988
- Computer Misuse Act 1990
- Education Act 1996; Education and Inspections Act 2006; Education Act 2011 (Part 2)
- Sexual Offences Act 2003
- Malicious Communications Act 1988 and Communications Act 2003
- Public Order Act 1986 and Equality Act 2010
- Obscene Publications Act 1959; Criminal Justice and Immigration Act 2008
- Criminal Justice and Courts Act 2015 (disclosing private sexual images without consent)
- Counter-Terrorism and Security Act 2015 (the Prevent duty)
- Voyeurism (Offences) Act 2019
- UK General Data Protection Regulation and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- Online Safety Act 2023
- Children's Wellbeing and Schools Act 2026 — section 36 requires state-funded schools in England to have regard to published guidance on mobile phones, and came into force on 29 June 2026

Statutory and non-statutory guidance

- DfE (2026) 'Keeping Children Safe in Education 2026' — in force from 1 September 2026
- DfE (2026) 'Mobile phones in schools' — updated January 2026 and given statutory force from 29 June 2026
- DfE 'Filtering and monitoring standards for schools and colleges' — updated June 2026 to address generative AI
- DfE 'Meeting digital and technology standards in schools and colleges', including the cyber security and IT support standards
- DfE 'Generative artificial intelligence (AI) in education' policy paper and 'Using AI in education settings: support materials'

- DfE ‘Generative AI: product safety expectations’
- DfE ‘Teaching online safety in schools’
- DfE ‘Searching, screening and confiscation: advice for schools’
- DfE ‘Harmful online challenges and online hoaxes’
- DfE ‘Behaviour in schools’ and ‘Preventing and tackling bullying’
- DfE ‘Relationships education, relationships and sex education (RSE) and health education’ statutory guidance
- UKCIS ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- UKCIS ‘Education for a Connected World’ framework
- UK Safer Internet Centre ‘Appropriate Filtering and Monitoring’ definitions (2026)
- Home Office ‘Prevent duty guidance: England and Wales’ and the Derbyshire Prevent pathway
- Derby and Derbyshire Safeguarding Children Partnership (DDSCP) procedures, including section 1.7.17 Online Safety and Internet Abuse
- National Cyber Security Centre ‘Cyber security for schools’ guidance
- JCQ ‘AI use in assessments: protecting the integrity of qualifications’ (where relevant to examined courses)
- Information Commissioner’s Office guidance on children’s data, AI and data protection

Off-site conduct and searching

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside school but are linked to membership of the school.

The DfE’s Searching, screening and confiscation guidance sets out the powers available to schools in relation to searching for and of electronic devices, and the examination and deletion of data. Any search of an electronic device will be carried out in line with that guidance and our Behaviour Policy, by staff authorised by the headteacher, with a second member of staff present wherever possible, and will be recorded.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school.

3. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school. All staff are expected to report searching for inappropriate content, any indication that a device in school may not have working filtering or monitoring, and any surge in searching on topics that may indicate risk or risky behaviour.

Trustees

- Ensure the trust has a robust online safety policy for the family of Embark schools, and that it is current and in line with national policy and guidance.
- Ensure this trust-wide policy is approved centrally in accordance with the Trust's Scheme of Delegation, and that local governing teams know about the policy and assure themselves that it is implemented effectively in their schools.
- Receive an annual report on online safety across the trust, including filtering and monitoring assurance, incident trends and training completion.
- Ensure that online safety, cyber security and data protection risks are recorded on the trust risk register and reviewed at least annually.

Governors

Local governing teams are responsible for receiving this trust-wide policy, assuring themselves that it is implemented effectively in their school and reviewing the effectiveness of local arrangements. This will be supported by regular information about online safety incidents and monitoring reports from the headteacher and DSL, and by assurance that the school is meeting the DfE's digital and technology standards. Formal approval of the trust-wide policy sits centrally in accordance with the Trust's Scheme of Delegation.

A member of the governing team takes on the role of Safeguarding Governor. The role includes:

- Regular meetings with the DSL and the IT Lead
- Regular monitoring of online safety incident logs and of trend data
- Regular monitoring of filtering and change control logs
- Reviewing and signing off the annual online safety risk assessment and the annual filtering and monitoring effectiveness review
- Reporting to the relevant governor board, committee or meeting
- Assuring themselves that governors and trustees have completed online safety and Prevent training

Governing bodies must ensure that appropriate filtering and monitoring systems are in place, that their effectiveness is reviewed at least once every academic year, and that the school can demonstrate that these reviews have taken place.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety, including online safety, of members of the school community, though day-to-day responsibility for online safety is delegated to the Designated Safeguarding Lead.
- A named member of the senior leadership team holds strategic responsibility for filtering and monitoring and leads the annual effectiveness review, supported by the DSL, IT Lead and trust IT service. Where the DSL is the named SLT lead, they lead the review in that capacity.

- The headteacher and at least one other member of the SLT are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see the flow chart at Appendix 3 and the trust's Managing Allegations and Concerns policy).
- The headteacher and SLT ensure that relevant staff receive suitable training to enable them to carry out their online safety roles and to train colleagues as relevant, including awareness of cyber threats and cybercrime.
- The headteacher and SLT ensure there is a system in place for the monitoring and support of those who carry out the internal online safety monitoring role, providing both a safety net and support to colleagues in those roles.
- The headteacher and Online Safety Governor receive regular audit and monitoring reports and use these to identify risks, trends and activities.
- The headteacher is responsible for the overall content of the school website, ensuring it is appropriate, accurate, up to date and meets government requirements.
- The headteacher ensures the school's mobile phone policy is implemented consistently and is understood by staff, students and parents.

Designated Safeguarding Lead (DSL) and deputies

- The DSL takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place.
- The DSL oversees and acts on filtering and monitoring reports, safeguarding concerns, and checks to filtering and monitoring systems.
- The named member of SLT with strategic responsibility for filtering and monitoring leads the annual review of effectiveness, supported by the DSL, IT Lead and trust IT service. Where the DSL is the named SLT lead, they lead the review in that capacity. The outcome is recorded and reported to governors.
- The DSL determines what is monitored, how alerts are triaged, and the timescales within which the school will respond to alerts, including out of hours and during holidays.
- The DSL undertakes training in online safety at least every two years, including cyber safety and security, and receives regular updates.
- The DSL ensures online safety concerns are recorded on the school's safeguarding recording system and analysed for patterns.

DSLs should be alert to the potential for serious safeguarding issues to arise from:

- Searching by students for materials, sites or platforms that may be harmful or misleading
- Sharing of personal data
- Access to illegal or inappropriate material
- Inappropriate online contact with adults or strangers
- Potential or actual incidents of grooming
- Online bullying, online hate and harmful sexual behaviour
- Interactions with AI chatbots, companion apps and other generative AI tools

IT Lead and technical staff

The IT Lead, supported by the trust's IT service, is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any local guidance that may apply.

- That users may only access networks and devices through properly enforced authentication, including multi-factor authentication where appropriate.
- That the filtering process is applied and updated regularly, and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to carry out their role effectively and to inform and update others.
- That use of the network, internet, remote access and email is regularly monitored so that any misuse or attempted misuse can be reported to the headteacher, DSL and Online Safety Governor for investigation, action or sanction.
- That monitoring software and systems are implemented and updated as agreed in school policies.
- That the technical capabilities and limitations of the filtering and monitoring provision are documented and shared with the DSL, including what the systems can and cannot see in relation to AI-generated content, encrypted traffic and mobile apps.
- That software licence logs are accurate and up to date, and that regular checks reconcile licences purchased against installations.

The management of technical security is the responsibility of the IT Lead, working with the trust IT service.

Teaching and support staff

Teaching and support staff are responsible for ensuring that:

- They have up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the Embark Trust Acceptable Use of the Internet and Electronic Communication agreement.
- They report any suspected misuse or problem to the DSL, headteacher and IT Lead for investigation, action or sanction.
- All digital communication with students, parents and carers is professional in tone and content and is carried out only using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- They monitor the use of digital technologies, mobile devices and cameras in school and other activities and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use, and processes are in place for dealing with any unsuitable material found in searches.
- They identify students who are involved in cybercrime, or who are technically gifted and at risk of becoming involved in cybercrime, and report concerns to the DSL.
- The curriculum recognises misinformation, disinformation and conspiracy theories as a significant online harm.
- Any generative AI tool used with or on behalf of students is on the school's approved list, and outputs are checked before use.

Students

- Are responsible for using school digital technology systems in accordance with the Student Acceptable Use Agreement.
- Have a good understanding of research skills, and of the need to avoid plagiarism and to uphold copyright — including when using generative AI.

- Understand the importance of reporting abuse, misuse or access to inappropriate materials, and know how to do so.
- Know and understand policies on the use of mobile devices and digital cameras, on the taking and use of images, and on online bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school, and that this policy covers their actions out of school where they are related to their membership of the school.
- Are expected to sign an age-appropriate Acceptable Use Agreement (Appendix 1).

Parents and carers

Many parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in monitoring and regulating their children's online behaviour. Parents may underestimate how often children come across potentially harmful and inappropriate material online, and may be unsure how to respond. The school will take every opportunity to help parents understand these issues, through:

- Curriculum activities and shared learning
- Letters, newsletters, the website and physical resources
- Parent and carer evenings and workshops, including sessions on generative AI, age ratings and home filtering
- High-profile events and campaigns, for example Safer Internet Day
- Reference to relevant websites and publications

Parents will be informed of this policy through the Acceptable Use Agreement and through online safety awareness sessions and newsletters. Information about keeping children safe online will be published on the school website, along with details of organisations where online abuse can be reported. All school websites carry the CEOP report abuse link.

We also ask parents and carers to:

- Support the school's mobile phone policy and reinforce it at home.
- Follow the school's expectations on taking and sharing photographs and video at school events (see Section 11).
- Use class or year group messaging apps responsibly, and raise concerns with the school directly rather than through social media.
- Contact the school promptly where an online incident involving students has arisen outside school, so that we can offer support and, where appropriate, act.

The wider community

The school will provide opportunities for local community groups and members of the community to benefit from the school's online safety knowledge and experience. This may include:

- Providing family learning in the use of digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents
- Partnership work with local schools
- Online safety information for the wider community on the school website
- Supporting community groups — for example early years settings, youth, sports and voluntary groups — to enhance their online safety provision

Visitors, contractors and external providers

- Visitors and contractors requiring network access are given time-limited guest access only, and are made aware of the relevant parts of this policy.
- External providers delivering activities to students — including online tutoring, remote clubs and visiting speakers — are subject to the school's due diligence checks, and must confirm their own safeguarding and online safety arrangements before working with students.
- Visitors are asked not to take photographs or video on personal devices while on site, other than where the headteacher has agreed this in advance.

4. The Prevent duty, radicalisation and extremism

There are specific roles and responsibilities set out in the Prevent duty guidance for England and Wales, which covers the possibility of online radicalisation and access to terrorist and extremist material.

- All staff, including trustees and governors, will receive training that incorporates online safety and the Prevent duty.
- All reasonable precautions will be taken to ensure that students and staff are safe from terrorist and extremist material when accessing the internet on the school site, and this forms part of the filtering risk assessment.
- If there are concerns that a student, parent, carer or member of the local community may be at risk of radicalisation online, the headteacher, SLT or DSL will be informed immediately and action will be taken in line with our Child Protection Policy and the Derbyshire Prevent pathway, which may include a referral into Channel where the person is a child or young person.
- If there are concerns that a member of staff, or a person working on behalf of the school, may be at risk of radicalisation online, the headteacher will be informed immediately and action taken in line with local child protection procedures and, where relevant, the Embark Trust Managing Allegations and Concerns policy.
- Staff will be alert to the ways in which extremist and misogynistic content is spread through mainstream platforms, recommendation algorithms, gaming and short-form video, rather than only through overtly extremist sites.

5. Education and training

Students

While regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. Children and young people need the help and support of the school to recognise and avoid online safety risks and to build their resilience.

Online safety is a focus in all areas of the curriculum, and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad and relevant, provides progression, and includes opportunities for creative activities. It is delivered in the following ways:

- A planned online safety curriculum is provided as part of computing, RSHE/PSHE and other lessons, and is regularly revisited.
- Key online safety messages are reinforced through a planned programme of assemblies and tutorial or pastoral activities.
- Students are taught in all lessons to be critically aware of the materials and content they access online and are guided to validate the accuracy of information, including content produced by generative AI.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed online.
- Students are helped to understand the need for the Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable, and processes are in place for dealing with unsuitable material found in searches.
- Where students are allowed to search freely, staff are vigilant in monitoring the content of the websites the students visit.
- The curriculum is mapped against the UKCIS ‘Education for a Connected World’ framework and reviewed annually against the risks identified in the school’s online safety risk assessment.

It is accepted that from time to time, for good educational reasons, students may need to research topics — for example racism, drugs or discrimination — that would normally result in internet searches being blocked. In such a situation, staff can request that technical staff temporarily remove those sites from the filtered list for the period of study. Any such request must be auditable, with clear reasons recorded for the need, and must be time-limited.

Students will be made aware of the importance of filtering systems through the online safety education programme, and warned of the consequences of attempting to subvert them.

Vulnerable students

Some students are at greater risk of harm online. We take account of this in both our curriculum and our risk assessment, recognising that students with special educational needs and disabilities, students with social, emotional and mental health needs, children with a social worker, looked-after and previously looked-after children, young carers, and students for whom English is an additional language may:

- Find it harder to recognise risk, manipulation or coercion online
- Be more likely to be targeted for grooming, exploitation or bullying
- Need differentiated or repeated teaching, or communication in an alternative format
- Require an individual risk assessment or personalised filtering and monitoring arrangements

The DSL and SENCO work together to ensure online safety education is accessible and that individual plans reflect online risk where relevant.

Student voice

- Students are surveyed at least annually about their online experiences, and the results inform the online safety curriculum and risk assessment.
- Digital leaders or online safety ambassadors, where appointed, help shape messages and support peers.
- Students are consulted on how easy it is to report a concern, and reporting routes are adjusted where they are not working.

Staff and volunteers

It is essential that all staff receive online safety training and understand their responsibilities as outlined in this policy. Training is provided as follows:

- A planned programme of formal online safety training is made available to staff, regularly updated and reinforced. An audit of the online safety training needs of all staff is carried out regularly.
- All new staff receive online safety and NCSC cyber security training as part of their induction, ensuring they fully understand this policy and the Acceptable Use Agreements.
- Training includes the safe use of AI tools, cyber security, recognising phishing, and the identification and reporting of online harms. It is updated at least annually via the trust's training platform and aligned with the latest statutory guidance.
- All staff read and understand Part One of Keeping Children Safe in Education in full. From September 2026 the shortened Annex A version is withdrawn.
- The DSL receives regular updates through attendance at external training events and by reviewing guidance released by relevant organisations.
- This policy and its updates are presented to and discussed by staff in staff meetings.
- The DSL provides advice, guidance and training to individuals as required.
- Staff who review monitoring alerts receive specific training on doing so, and are supported given the nature of the content they may see.

Governors and trustees

Governors should take part in online safety training or awareness sessions, which is of particular importance for those who are members of any group involved in technology, online safety, health and safety or child protection. This may be offered through:

- Attendance at training provided by the Embark Trust, which may be delivered online
- Participation in school training or information sessions for staff or parents, which may include attendance at assemblies or lessons
- Use of the UKCIS 'Online safety in schools and colleges: questions from the governing board' as a self-assessment tool

6. Technical infrastructure, filtering and monitoring

Governing bodies and proprietors should do all that they reasonably can to limit children's exposure to online risks from the school's IT system, and must ensure the school has appropriate filtering and monitoring systems in place. In considering their responsibility to safeguard and promote the welfare of children, governing bodies should consider the age range of their students, the number of students, how often they access the IT system, and the proportionality of costs against risks.

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The trust uses L.E.A.D. IT Services to provide a complete system and set of technologies that help keep students and staff safe across the Embark family of schools.

Infrastructure and access

- School technical systems are managed in ways that ensure the school meets recommended technical requirements.
- There are regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school technical systems and devices, recorded by the IT Lead and reviewed at least annually with the DSL.
- Users can only access data to which they have a right of access, and no user is able to access another's files other than as allowed for monitoring purposes within school policy.
- Access to personal data is securely controlled in line with the trust's data protection policy.
- Logs are maintained of user access and of user actions on the system.
- The master or administrator credentials for school systems are also available to the headteacher or another nominated senior leader and are kept securely; no single individual holds sole administrator access.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff.
- Mobile device management is in place for school devices, and device security procedures apply where devices are permitted to access school systems.
- An agreed process is in place for the provision of temporary, time-limited access for guests such as trainee teachers, supply teachers and visitors.
- Staff are not permitted to download executable files or install programmes on school devices.
- Remote management tools are used by authorised staff to support devices and, where necessary, view user activity; users are made aware of this in the Acceptable Use Agreement.
- An appropriate route is in place for users to report any actual or potential technical incident or security breach.
- Personal data is not sent over the internet or taken off site unless safely encrypted or otherwise secured.

Filtering

The filtering of internet content is an important means of preventing users from accessing material that is illegal or inappropriate in an educational context. No filtering system can provide a 100% guarantee: web content changes dynamically and new technologies emerge constantly. Filtering is therefore only one element in a wider strategy for online safety and acceptable use, and the school demonstrates that it has taken all other reasonable precautions.

- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider, which actively employs the Internet Watch Foundation CAIC list and other illegal content lists.
- Content lists are regularly updated, internet use is logged, and use is frequently monitored.
- The school provides enhanced, differentiated, user-level filtering, so that filtering is appropriate to the age and role of the user.
- Filtering applies to all devices that access the school internet connection, including personal devices where these are permitted, and to school devices used off site.
- Filtering is applied without over-blocking, so that it does not unreasonably impact teaching and learning or restrict students from accessing age-appropriate support, including on health, identity and wellbeing.
- Users must not attempt to use any programme, VPN, proxy or other software that might allow them to bypass filtering or security systems.
- All users have a responsibility to report immediately to the IT Lead any infringements of the filtering of which they become aware, or any sites that are accessed which they believe should have been filtered.
- Filtering must be capable of, or supplemented to address, real-time, dynamic, personalised and AI-generated content. Where DNS or URL-based filtering cannot detect risk inside AI-generated material, this limitation is documented and mitigated through monitoring, supervision and education.

Changes to the filtering system

To ensure there is a system of checks and balances, and to protect those responsible, changes to the school filtering service must:

- Be requested through the agreed route, with a clear educational or operational reason recorded
- Be authorised by a second responsible person — ordinarily the headteacher or DSL — prior to the change being made
- Be logged in change control logs, including who requested, who authorised, what changed and for how long
- Be time-limited where the change is for a specific period of study, and reversed at the end of that period

In the event that technical staff need to switch off filtering for any reason, or for any user, this must be logged and carried out through a process agreed by the headteacher. Any filtering fault or gap must be reported immediately to the filtering provider.

Monitoring

Monitoring is distinct from filtering: filtering restricts what can be reached, while monitoring identifies concerning behaviour so that the school can respond. The DSL is responsible for determining what is monitored and for the response to alerts.

- School technical staff regularly monitor and record the activity of users on school technical systems, and users are made aware of this in the Acceptable Use Agreement.
- Monitoring covers school devices in and out of school, and school accounts accessed on any device, to the extent technically possible.
- Automated weekly reports are emailed to DSLs for review, and higher-risk alerts are escalated immediately.

- The DSL sets and records expected response timescales for different alert categories, including arrangements for evenings, weekends and school holidays.
- Monitoring is proportionate, transparent to staff, students and parents, and carried out in line with data protection requirements.
- All concerns identified through monitoring are recorded on the school's safeguarding recording system and managed under the Child Protection and Safeguarding Policy, not solely as a behaviour matter.
- Logs identify the individual user, so that the school can respond to a concern about a specific child.

Annual review of effectiveness

Keeping Children Safe in Education 2026 requires schools to review the effectiveness of their filtering and monitoring systems at least once every academic year, and to be able to demonstrate that this has happened.

- The review is led by the named member of the senior leadership team with strategic responsibility for filtering and monitoring, supported by the DSL, IT Lead and trust IT service. Where the DSL is the named SLT lead, they lead the review in that capacity.
- It considers the risk profile of the school's students, what the systems block and detect, what they cannot see, how alerts are triaged and acted on, and whether provision remains proportionate as technology changes.
- It includes practical testing of blocking and keyword detection, using tools such as those provided by the UK Safer Internet Centre, checking that testing does not impact teaching and learning.
- It explicitly considers whether the provision can handle real-time, dynamic, personalised and AI-generated content, and whether any generative AI tools introduced since the last review have been risk assessed.
- The outcome is recorded in writing, retained as evidence, reported to governors, and used to produce an action plan with named owners and dates.
- A filtering risk assessment is completed per school and signed off annually by the Online Safety Governor.

Logs of filtering change controls and of filtering incidents are made available to the headteacher, the DSL, the Online Safety Governor, and to the filtering provider, local authority or police on request.

DfE filtering and monitoring standards: gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

7. Cyber security and digital resilience

Schools hold some of the most sensitive personal data in the public sector and are an active target for ransomware and phishing attacks. A successful attack can disrupt learning, compromise student and staff data, and create safeguarding risk. The trust therefore treats cyber security as part of, not separate from, online safety.

The school works towards the DfE's cyber security standards and the NCSC's guidance for schools. In practice this means:

Technical controls

- Multi-factor authentication is enabled on all accounts where it is available, and is mandatory for administrator, finance, MIS and safeguarding system accounts.
- Operating systems, applications and browsers are kept up to date, with a defined patching schedule and a route for emergency patches.
- Anti-malware protection is deployed on all devices, and firewalls are properly configured on every network.
- Accounts follow least-privilege principles; administrator accounts are separate from day-to-day accounts and are reviewed regularly.
- A documented joiners, movers and leavers process ensures accounts and access are created, amended and revoked promptly, and leavers' access is removed on their last day.
- Backups are taken regularly, tested for restoration at least annually, and at least one copy is held offline or otherwise isolated from the network.
- Remote access is secured and logged.

People and process

- All staff and governors complete cyber security training, including phishing awareness, at induction and at least annually.
- Staff are expected to report suspected phishing, unusual account activity or lost devices immediately to the IT Lead — reporting quickly is always the right response, and staff will not be penalised for reporting a mistake.
- The school has a cyber incident response and business continuity plan setting out who does what, how the school will operate without IT, and how it will communicate with parents and staff.
- Suppliers and third-party services are subject to due diligence, including data protection and security assurance, before deployment; Cyber Essentials certification is expected of key suppliers where proportionate.
- A register of systems and services holding personal data is maintained, with a named owner for each.

Incident reporting

- Suspected cyber incidents are reported immediately to the headteacher, IT Lead and trust IT service.
- A personal data breach is reported to the trust Data Protection Officer without delay, and, where it meets the threshold, to the Information Commissioner's Office within 72 hours of the school becoming aware of it.
- Criminal cyber incidents are reported to Action Fraud, and significant incidents to the NCSC; the DfE is notified where required.

- Where an incident has safeguarding implications — for example the loss of safeguarding records, or unauthorised access to student data — the DSL is involved from the outset.
- Cyber incidents and near misses are logged and reviewed, and lessons learned are fed into training and the annual risk assessment.

Students and cybercrime

We respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even where this takes place off site. Where a child appears to be being exploited because of their technical skills, we follow the Children at Risk of Exploitation procedure. Staff will consider a referral to the National Crime Agency's Cyber Choices programme as an early intervention where appropriate, rather than treating technically able students solely as a behaviour issue.

8. Password security and access management

A safe and secure username and password system is essential and applies to all school technical systems, including networks and devices. Our approach follows National Cyber Security Centre advice, which prioritises password length, uniqueness and multi-factor authentication over frequent forced changes.

All users

- All users have clearly defined access rights to school technical systems and devices. Details of access rights available to groups of users are recorded by the IT Lead and reviewed with the DSL.
- All school networks and systems are protected by secure passwords.
- Users are responsible for the security of their username and password, must not allow other users to access systems using their log-on details, and must immediately report any suspicion or evidence of a breach of security.
- Passwords must be different for different accounts, so that other systems are not put at risk if one is compromised, and must be different for systems used inside and outside school.
- Requests for password changes are made via the IT Lead.

Staff passwords

- All staff are provided with a username and password by the IT Lead, who keeps an up-to-date record of users and their usernames.
- Passwords should be long and memorable — the NCSC ‘three random words’ approach is recommended — and must not include proper names or other personal information about the user that might be known to others.
- Multi-factor authentication is applied to school accounts wherever available, and is mandatory for privileged accounts.
- Passwords are not routinely expired on a fixed cycle. A change is enforced where there is any suspicion of compromise, where a shared credential has been used, or where a member of staff leaves a role with privileged access. Where a system requires periodic change, the interval will be no shorter than is operationally necessary.
- Common, previously breached and easily guessed passwords are blocked where the system supports it, and staff are encouraged to use an approved password manager.
- Accounts are locked out following repeated incorrect log-on attempts.
- Temporary passwords, for example for new accounts or resets, must be changed on first log-on.
- Passwords are not displayed on screen and are stored securely hashed.
- Staff must not write down or share passwords, and must not save school passwords in personal browsers or on personal devices.

Student passwords

- All students at KS2 and above are provided with a username and password by the IT Lead, who keeps an up-to-date record of users and their usernames.
- Password complexity is set with regard to the cognitive ability and age of the children.
- Students are taught the importance of password security and of not sharing passwords, including with friends.
- Student passwords are changed where there is any concern about misuse or where an account may have been accessed by another student.

Training, audit and review

Staff are made aware of the school's password procedure at induction, through this policy and through the Acceptable Use Agreement. Students are reminded of the importance of not sharing passwords in lessons and through the Acceptable Use Agreement.

The IT Lead ensures that full records are kept of user IDs and requests for password changes, user log-ons, and security incidents related to this policy.

9. Generative artificial intelligence (AI)

Generative AI can support teaching, reduce workload and improve accessibility. It also introduces risks around safeguarding, data protection, academic integrity and the reliability of information. Keeping Children Safe in Education 2026 identifies AI within both the contact and conduct risk categories, and the school treats AI as a managed education tool rather than a shortcut around professional responsibility.

The school will take steps to prepare students for changing and emerging technologies, including generative AI, and how to use them safely and appropriately, with consideration given to students' age.

Approval and assurance of AI tools

- Only AI tools on the school's approved list may be used with students or with school data. Requests for new tools are made to the IT Support Team for approval and set-up (see the checklist at Appendix 5).
- A Data Protection Impact Assessment is completed before any AI tool that processes personal data is deployed, and is logged centrally with the trust Data Protection Officer.
- Tools are assessed against the DfE's Generative AI: product safety expectations, covering filtering, monitoring, content safety, transparency, data protection, intellectual property and testing.
- Age limits set by the provider are respected. Where a tool's terms require users to be 13 or 18, it will not be used directly by students below that age.
- The approved list is reviewed at least annually, and as part of the annual filtering and monitoring effectiveness review.

DfE Generative AI: product safety expectations — gov.uk/government/publications/generative-ai-product-safety-expectations

Filtering, monitoring and AI

- The school ensures its IT systems include filtering and monitoring appropriate to limiting students' ability to access or create harmful or inappropriate content through generative AI.
- The June 2026 update to the DfE Filtering and Monitoring Standards brings AI-generated content explicitly within the scope of filtering, and asks schools to consider whether their provision can handle real-time, dynamic, personalised and AI-generated content. The school documents its technical limitations in this area and mitigates them.
- Monitoring systems should maintain logging of interactions with AI tools where technically possible, and the DSL is made aware of what can and cannot be seen.
- AI chatbots, companion apps and character-based AI services are treated as a contact risk. Staff are alert to students forming attachments to, or receiving harmful advice from, such services, and to their use as a route for grooming or for accessing harmful content.

Data protection and staff use

- Personal, sensitive or special category data must not be entered into generative AI tools. This includes student names, safeguarding information, SEND information, behaviour records, staff information and photographs of children.
- AI must not be used to draft or summarise safeguarding records, and AI note-takers or transcription tools must not be used in safeguarding, child protection, SEND or HR meetings unless specifically approved with a completed DPIA.
- Staff remain professionally responsible for any output they use. AI supports but does not replace professional judgement, and must not make unsupervised decisions about students, including on assessment, attainment, behaviour or safeguarding.

- All AI-generated content used in school must be checked for accuracy, bias and appropriateness before use with students.
- Where AI has been used to help produce material shared with parents or published, staff apply the same standards of accuracy and professionalism as for any other school communication.

Students, teaching and academic integrity

- Students are taught about the risks of AI-generated content — misinformation, deepfakes, bias, privacy, profiling and persuasive design — and are taught the critical thinking skills needed to identify fake news and conspiracy theories.
- Students are taught that AI can be confidently wrong, that it reflects the biases of its training data, and that anything they type into it may be stored or used by the provider.
- Expectations on the use of AI in homework and assessed work are made clear to students and parents. Where students are entered for external qualifications, JCQ requirements on AI use in assessments apply and are reflected in the school's malpractice arrangements.
- The creation of sexual, abusive, harassing or discriminatory content using AI — including so-called 'nudify' apps and deepfakes of students or staff — is treated as a serious safeguarding and behaviour matter and is dealt with under Sections 12 and 18 of this policy.
- The positive and accessible uses of AI, including for students with SEND, are recognised and supported where the tool is approved.

Training and information

- All staff receive regular training on the safe use of AI tools, the risks of bias, misinformation and data privacy, and how to report concerns. Training is updated at least annually via the trust's training platform.
- Governors and trustees receive updates on AI, filtering and monitoring, and the outcomes of online safety audits.
- The school provides parents and carers with information about the risks associated with AI, including misinformation, chatbots and data privacy, and how to support children in navigating AI-generated content. Resources are shared through newsletters, workshops and the school website.

10. Mobile phones and personal devices

The DfE's Mobile phones in schools guidance was updated in January 2026 and states that all schools should be mobile phone-free environments by default, with anything other than this by exception only. Section 36 of the Children's Wellbeing and Schools Act 2026, in force from 29 June 2026, requires schools to have regard to that guidance, giving it the force of law. Ofsted evaluates schools' mobile phone policies and their implementation as part of inspection.

Students

- Students do not have access to mobile phones throughout the school day — including lessons, the time between lessons, breaktimes and lunchtimes.
- The same expectation applies to other smart technology with similar functionality, including smart watches, smart glasses and devices that can message, browse, record, take photographs or receive notifications. Wireless earbuds are also covered.
- The practical arrangements for how this is achieved — for example phones handed in on arrival, or secured in a locked pouch or locker — are set out in the school's Behaviour Policy, which each school applies according to its context and phase.
- Where a device is brought into school contrary to this policy, staff may confiscate it in line with the Behaviour Policy and the DfE's searching, screening and confiscation guidance. Students may be searched for a mobile phone where the school has reasonable grounds.
- Sanctions for breaches are proportionate, applied consistently, and set out in the Behaviour Policy.

Exceptions and reasonable adjustments

Exceptions are made by the headteacher, are recorded, and are reviewed. They will be considered where a student:

- Has a medical need — for example where a phone is used to monitor blood glucose — or another health condition requiring continuous access
- Has a disability or special educational need where access to a device is part of their agreed support
- Has an exceptional personal or safeguarding circumstance, such as caring responsibilities

Reasonable adjustments will be made in line with the Equality Act 2010, and the school will discuss arrangements with the student and their parents or carers. Assistive technology provided by the school for a student's learning needs is not affected by this section.

Journeys, trips and residentials

- The policy applies to the school day. For educational visits, the visit leader makes an active, documented decision about whether phones are permitted, weighing the risks and any benefits, and ensures that the educational experience is not disrupted.
- Where phones are permitted on a residential, expectations about photography, social media posting and night-time use are agreed and shared with students and parents in advance.

Staff, volunteers and visitors

- Staff should not use personal mobile phones where they are responsible for the supervision of students, other than in an emergency or with the agreement of a senior leader.
- Personal devices must not be used to photograph or record students, or to contact students or parents (see Sections 11, 14 and 15).
- Staff model the behaviour expected of students.

- Visitors and contractors are asked to keep personal phone use out of areas where students are present, and not to photograph or record students.

Communicating the policy

- The policy is published on the school website and shared with parents at the start of each academic year and on admission.
- Parents are asked to contact the school office, not their child directly, if they need to pass on a message during the school day.
- Staff apply the policy consistently, and the SLT monitors implementation and reports to governors.

11. Use of digital and video images

Digital imaging technologies bring significant benefits to learning, allowing staff and students instant use of images they have recorded or accessed. However, staff, parents, carers and students need to be aware of the risks associated with publishing digital images online. Such images may provide avenues for online bullying. Digital images may remain available online indefinitely and may cause harm or embarrassment in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement measures to reduce the potential for harm.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, students should recognise the risks attached to publishing their own images online, including on social networking sites.
- Staff and volunteers may take digital and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images should only be taken on school equipment; the personal equipment of staff must not be used for such purposes. Photographs should be uploaded to the secure staff shared area and erased from any portable devices.
- Care should be taken when taking images that students are appropriately dressed and are not participating in activities that might bring individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website or social media channels, and consent is recorded, reviewed and can be withdrawn at any time.
- Students' work can only be published with the permission of the student and their parents or carers.
- Where a student has a specific safeguarding reason for not being photographed, arrangements are recorded and communicated to relevant staff, including for events, displays and the media.

Parents and carers at school events

In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use, as such use is not covered by data protection law. To respect everyone's privacy, and in some cases their protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other students in the digital or video images.

> *Schools will inform parents and carers if they need to restrict photographs or videos from being taken at school events. It may not always be possible to explain why the decision has been made if there are confidential concerns, but it will not have been taken without good reason. In these circumstances, schools will endeavour to share pictures with parents and carers after the event.*

Livestreaming of school events by parents or carers, and the posting of footage of other people's children, is not permitted.

12. Nudes and semi-nudes (including AI-generated and altered images)

The sharing of nudes and semi-nudes is one of a number of risk-taking behaviours associated with the use of digital devices, social media and the internet. It is accepted that young people experiment and challenge boundaries, and that the risks associated with online activity can never be completely eliminated. The school takes a proactive approach to helping students understand, assess, manage and avoid those risks, and recognises its duty of care to students who find themselves involved in such activity, as well as its responsibility to report where legal or safeguarding boundaries are crossed.

Definition

For the purposes of this policy, this means:

- Images or videos of children under the age of 18 that are of a sexual nature or are indecent, generated by or of those children
- Images that have been digitally altered, or wholly generated using AI, to depict a child in a nude or semi-nude state — including images created using so-called ‘nudify’ apps
- Such images shared between young people, or between young people and adults, via any device, platform or service

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Crimes involving indecent photographs, including pseudo-images, of a person under 18 fall under Section 1 of the Protection of Children Act 1978 and Section 160 of the Criminal Justice Act 1988. Under this legislation it is a crime to:

- Take an indecent photograph, or allow an indecent photograph to be taken
- Make an indecent photograph — this includes downloading or opening an image sent by email or message
- Distribute or show such an image
- Possess such an image with the intention of distributing it
- Advertise or possess such images

It is rare for the police to prosecute child-on-child incidents, and they will always consider the circumstances, including power, control, coercion, ages and any exploitation. The existence of Outcome 21 means that a young person may be recorded as having committed a crime without it appearing on future criminal records checks in most circumstances.

Responding to an incident

All incidents involving the sharing of nude or semi-nude images require a safeguarding response, whether the sharing appeared consensual or non-consensual.

The school follows the UKCIS guidance ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’, and the local procedures set out by the Derby and Derbyshire Safeguarding Children Partnership (section 1.7.17, Online safety and internet abuse).

Sharing nudes and semi-nudes: advice for education settings (GOV.UK)

DDSCP — Online Safety and Internet Abuse procedures

Staff must always

- Report the incident to the DSL (or deputy DSL) immediately — the DSL takes any necessary strategic decisions.
- Record the incident on the school’s safeguarding recording system.
- Act in accordance with the school’s safeguarding, search and confiscation policies and procedures.

- Store any device securely, without deleting anything from it.

Staff must never

- View, copy, print, share, store or forward the image or video. If a staff member has already viewed an image by accident or before realising what it was, this must be reported to the DSL and recorded.
- Ask a child to share or unlock a device so that the image can be seen.
- Delete the image or ask the child to delete it before the DSL has decided on the response.
- Ask a child to disclose information about the image in front of other children, or say or do anything that blames or shames any child involved.
- Promise confidentiality to the child.

The only circumstances in which an adult should view an image are set out in the UKCIS guidance, and any such decision must be made by the DSL, recorded, and taken by a member of staff of the same sex as the child wherever possible.

Disclosure by a student

Disclosures should follow the normal safeguarding practices and protocols set out in the Child Protection and Safeguarding Policy. A student is likely to be very distressed, especially if the image has been circulated widely and they do not know who has shared it, seen it, or where it has ended up. They will need emotional support during the disclosure and afterwards. They may need immediate protection or a referral to police or children's social care; parents should be informed as soon as possible, police advice permitting.

The following questions help staff and the DSL decide on the best course of action:

- Is the student disclosing about receiving, sending or sharing an image?
- What sort of image is it, and is it potentially illegal or inappropriate?
- Was the image real, or digitally altered or AI-generated, and does the student know?
- How widely has the image been shared, and is the device in their possession?
- Is it a school device or a personal device?
- Does the student need immediate support or protection?
- Are other children or young people involved, and is there any indication of coercion, blackmail or an adult being involved?
- Do they know where the image has ended up?

Regardless of whom the initial disclosure is made to, that person must act in accordance with the Child Protection and Safeguarding Policy and ensure the DSL is involved. The DSL (or in their absence the deputy DSL) always records the incident and always informs the headteacher.

Deciding on a response

There may be many reasons why a student has shared an image — it may be sexual exploration, or it may be the result of coercion, exploitation or blackmail. It will not always be appropriate to inform the police, and this will depend on the nature of the incident, but incidents must be consistently recorded. Where a crime may have taken place, the police are the first port of call.

If indecent images of a student are found, staff will:

- Act in accordance with the Embark Trust Safeguarding and Child Protection Policy
- Store the device securely
- Support the DSL to carry out a risk assessment in relation to the young person

- Make a referral where necessary, and contact the police where appropriate

Referrals may be made to children's social care. Students involved in experimental sharing contained between two people may be referred to external agencies for support and guidance. Those who are victims will also be referred to children's social care at a point where the police confirm this will not impede an investigation. The DSL or deputy DSL will inform parents and carers about the incident and how it is being managed, and will offer support to the student.

Removing images

If an indecent image of a child is on a website or social networking site, the school will report it. Where a student may be at risk of abuse, the incident will be reported directly to CEOP at ceop.police.uk/safety-centre, so that law enforcement can assess the case, expedite it with the relevant provider and ensure appropriate action is taken to safeguard the child.

Two tools can help a young person have images removed. **Report Remove**, run by Childline and the Internet Watch Foundation, allows an under-18 in the UK to report a nude image or video of themselves for removal from the internet: childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online. NCMEC's **Take It Down** tool can be used to anonymously prevent the sharing of images that have not yet been circulated, for example where a young person has been threatened: takeitdown.ncmec.org.

Ongoing support

Students involved may be left feeling sensitive and vulnerable for some time and will require monitoring and support from a key worker or member of support staff. Where incidents become widespread, or where there is thought to be a possibility of contagion, the school will reinforce the need for safer online behaviour using a range of resources. Other staff may need to be informed and should be prepared to act if the issue continues or is referred to by other students.

Creating a supportive environment for students in relation to the incident is very important. The school, its students and parents should be alert, challenging behaviour and ensuring that the victim is well cared for and protected. Parents should usually be told what has happened so that they can keep a watchful eye over their child, particularly when they are online at home.

Preventative educational programmes can be found at CEOP's Thinkuknow website and through SWGfL's So You Got Naked Online resources. Support and guidance for staff, students, parents and carers is available from the NSPCC.

13. Other online harms

Online bullying and online hate

Online bullying is a form of bullying and will not be tolerated. Full details are set out in our Anti-Bullying Policy. Online hate content, whether directed at or posted by a member of the school community, will not be tolerated and will be responded to in line with existing policies, including the Anti-Bullying and Behaviour policies. The police will be contacted where a criminal offence is suspected.

Misogyny and harmful sexual behaviour

We are alert to the influence of online misogyny and of content that normalises sexual harassment, coercion or violence. Sexualised online behaviour between children — including unwanted sexual messages, the sharing of sexual images without consent, and sexual harassment carried out through group chats and social media — is treated as child-on-child abuse and is responded to under the Child Protection and Safeguarding Policy. Staff will not dismiss such behaviour as banter or as part of growing up.

Sextortion (financially motivated sexual extortion)

Sextortion is a rapidly growing risk affecting children of all ages, and boys in particular. It involves an offender — often part of an organised crime group operating from overseas — threatening to release sexual images of a young person unless money is paid.

- Students are taught that it is never their fault, that they should not pay, should not comply with further demands, should keep evidence, and should tell a trusted adult immediately.
- Staff who receive such a disclosure follow the safeguarding procedures in Section 12, report to the DSL immediately, and treat the child as a victim of crime.
- The DSL will report to the police and will consider the immediate risk of self-harm, given the acute distress and shame associated with these offences.
- Parents are provided with information about sextortion, including the warning signs.

Harmful online challenges and hoaxes

The school follows the DfE guidance ‘Harmful online challenges and online hoaxes’. We will not share unverified information about a challenge or hoax with students or parents, as this can increase reach and harm. Where a concern arises, the DSL will establish the facts, seek advice through the trust and local safeguarding partnership, and decide on a proportionate, age-appropriate response.

Self-harm, suicide and eating disorder content

We recognise that students may encounter, seek out or share content relating to self-harm, suicide or disordered eating. Filtering and monitoring are configured to identify such searches, and alerts are treated as safeguarding concerns requiring a same-day response. Staff responding will focus on the child’s wellbeing, avoid discussion of methods, and involve the DSL immediately. Support is offered in line with the school’s mental health and safeguarding arrangements, and the school will signpost students and families to appropriate services.

Misinformation, disinformation and conspiracy theories

These are recognised as significant online harms. They are addressed in the curriculum through media literacy, source evaluation and critical thinking, and staff are alert to the ways in which conspiracy content can act as a pathway towards extremism.

Gambling, loot boxes and financial harm

Students are taught about online gambling, gambling-style mechanics in games such as loot boxes, in-app purchasing, scams, phishing and fraudulent advertising. We are alert to signs that a student may be being recruited as a money mule, and will treat this as potential criminal exploitation.

Online criminal and sexual exploitation

We recognise that grooming for criminal exploitation, including county lines activity, and for sexual exploitation, frequently begins on social media and gaming platforms. Concerns are managed under the Child Protection and Safeguarding Policy and the Children at Risk of Exploitation procedure.

Gaming, livestreaming and connected devices

Students are taught about age ratings, in-game chat, livestreaming, connected toys and smart devices, and the risks of sharing personal information or being contacted by strangers through these routes. Parents are given information about parental controls and age ratings.

Cybercrime

Cybercrime incidents and offences are responded to in line with our behaviour policies and Section 7 of this policy.

14. Communications, remote learning and online meetings

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education to outweigh their risks and disadvantages. Student use of personal mobile phones and smart watches during the school day is covered by Section 10.

	Staff and other adults			Students		
Communication technologies	**Allowed**	**Allowed at certain times**	**Not allowed**	**Allowed**	**Allowed with staff permission**	**Not allowed**
Personal mobile phones and smart watches used during the school day		x				x
Use of personal devices in lessons			x			x
Taking photographs or video on personal phones or cameras			x			x
Use of school-owned mobile devices, e.g. tablets	x				x	
Use of personal email addresses in school, or on the school network		x				x
Use of school email for personal emails		x				x
Use of school-approved messaging apps		x			x	
Use of social media (official school accounts only)		x			x	
Use of blogs (school blogs only)		x			x	
Use of approved generative AI tools (see Section 9)	x				x	
Use of video broadcasting, e.g. YouTube		x			x	

Good practice in the use of communication technologies

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should use only the school email service to communicate with others when in school or on school systems, including by remote access.
- Users must immediately report to the nominated person the receipt of any communication that makes them feel uncomfortable, or that is offensive, discriminatory, threatening or bullying in nature, and must not respond to any such communication.

- Any digital communication between staff and students, parents or carers must be professional in tone and content and may only take place on official, monitored school systems. Personal email addresses, personal phone numbers, text messaging and social media must not be used.
- Whole class or group email addresses may be used at KS1, while students at KS2 and above may be provided with individual school email addresses for educational use.
- Students are taught about online safety issues such as the risks attached to sharing personal details, are taught strategies to deal with inappropriate communications, and are reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not posted on the school website, and only official email addresses are used to identify members of staff.
- Staff should not communicate with students or families outside working hours other than through official systems, and should be mindful of setting sustainable expectations about response times.

Remote learning and live online lessons

Where the school delivers learning remotely, the following apply:

- Only school-approved platforms are used, with school accounts and with recording, chat and screen-sharing settings configured appropriately for the age of the students.
- Live sessions are scheduled through school systems, and two members of staff attend, or the session is recorded, wherever practicable.
- One-to-one live sessions with a student take place only with the agreement of a senior leader, with parents informed in advance, and with the session recorded or a second adult present.
- Staff and students dress appropriately and use a neutral or blurred background, and sessions take place in an appropriate room rather than a bedroom wherever possible.
- Parents and carers are informed of the arrangements and are asked to supervise younger students.
- Recordings are stored securely in line with the trust's retention schedule and are not shared beyond the intended audience.
- The same behaviour and safeguarding expectations apply as in a classroom; concerns are reported to the DSL in the usual way.
- Where an external provider delivers online sessions, the school completes due diligence and remains responsible for the safeguarding arrangements.

15. Social media – protecting professional identity

All schools have a duty of care to provide a safe learning environment for students and staff. Schools and trusts may be held responsible, indirectly, for the acts of their employees in the course of their employment. Staff who harass, bully online, discriminate on the grounds of a protected characteristic, or defame a third party may render the school or trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to minimise the risk of harm to students, staff and the school through limiting access to personal information:

- Training covering acceptable use, social media risks, checking of privacy settings, data protection and reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Expectations of staff

In line with the Staff Code of Conduct, school staff should ensure that:

- No reference is made in social media to students, parents, carers or school staff.
- They do not post or communicate disparaging or defamatory statements, using social media or otherwise, about our employees, our governors, our learners and their parents and carers, our suppliers, agents and contractors, or our trustees.
- They do not make statements that could be construed as damaging or detrimental to the reputation of the school.
- They do not engage in online discussion on personal matters relating to members of the school community.
- They recognise that they are personally responsible for what they communicate via social media, and that what they publish might be read by a wider audience than they intended.
- Any social media communication is made on their own behalf and does not appear to be linked with the school in any way; personal opinions are not attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.
- They do not make contact with students on social networking sites. Any electronic or text communication is conducted through the school's systems and only where there is a clear and demonstrable school reason.
- They do not have current students, or those who have left less than six years ago, as online friends or contacts, except relatives. Where there is a legitimate reason for such contact, for example involvement with Scouts, a youth club or a sports team, this is declared to the headteacher and a copy of that organisation's safeguarding policy is provided.
- They do not use generative AI to create content about, or in the likeness of, students, colleagues or families.
- They report to the headteacher any online contact from a student or parent that is inappropriate, and any occasion on which they become aware that material about them or the school is circulating online.

These expectations apply whether social media is accessed using school facilities and equipment or equipment belonging to staff personally, and to the use of social media for both school and personal purposes, whether or not during working hours.

School social media accounts

- Official accounts are set up and administered only with the agreement of the headteacher, with at least two members of staff holding access.
- Content is checked before posting against the school's image consent records.
- Comments are moderated, and the school will not conduct discussions about individual students, staff or complaints on social media.
- Account credentials are managed under Section 8, and access is removed promptly when a member of staff leaves.

16. Data protection

Personal data will be recorded, processed, transferred and made available in line with the requirements and protections set out in the UK General Data Protection Regulation and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, which require that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that

- It holds the minimum personal data necessary to enable it to perform its function, and does not hold it for longer than necessary for the purposes for which it was collected (see the retention schedule).
- Every effort is made to ensure that data held is accurate and up to date, and that inaccuracies are corrected without unnecessary delay.
- All personal data is fairly obtained in accordance with the privacy notice and lawfully processed in accordance with the conditions for processing.
- It has a Data Protection Policy, is registered as a data controller, and has a Data Protection Officer for the trust.
- Data protection risk assessments and Data Protection Impact Assessments are carried out, including before the deployment of any new system, app or AI tool that processes personal data.
- There are clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for these to be exercised.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents, and reportable breaches are notified to the ICO within 72 hours.
- There are clear data protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage and cloud computing which ensure that such data storage meets the requirements set out by the Information Commissioner's Office.

Staff must ensure that they

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure, password-protected devices, ensuring they are properly logged off at the end of any session in which they are using personal data.
- Transfer data using encryption and secure, password-protected devices, and use school systems rather than personal accounts or storage.
- Do not enter personal, sensitive or special category data into generative AI tools (see Section 9).
- Report any actual or suspected data breach immediately, however minor it appears.

Removable media

Where personal data is stored on any portable computer system, memory stick or other removable media:

- The data must be encrypted and password protected.
- The device must be password protected, remembering that many memory sticks, cards and other mobile devices cannot be password protected — in which case they must not be used.
- The device must have approved virus and malware checking software available.
- The data must be securely deleted from the device, in line with school policy, once it has been transferred or its use is complete.

The use of removable media should be avoided wherever a secure school cloud service can be used instead.

17. Unsuitable and inappropriate activities

The school believes that the activities set out below would be inappropriate in a school context, and that users should not engage in them in school, or outside school when using school equipment or systems.

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, or make, post, download, upload, transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:					
Child sexual abuse images — the making, production or distribution of indecent images of children, contrary to the Protection of Children Act 1978. This includes images that are digitally altered or wholly AI-generated.					**x**
Grooming, incitement, arrangement or facilitation of sexual acts against children, contrary to the Sexual Offences Act 2003					**x**
Possession of an extreme pornographic image, contrary to the Criminal Justice and Immigration Act 2008					**x**
Criminally racist material, or material intended to stir up religious hatred or hatred on the grounds of sexual orientation, contrary to the Public Order Act 1986					**x**
Terrorist or violent extremist material, contrary to the Terrorism Acts 2000 and 2006					**x**
Disclosing private sexual images without consent,					**x**

contrary to the Criminal Justice and Courts Act 2015					
Pornography				**x**	
Promotion of any kind of discrimination				**x**	
Misogynistic content, or content promoting sexual harassment or coercion				**x**	
Threatening behaviour, including promotion of physical violence or mental harm				**x**	
Content promoting self-harm, suicide or disordered eating				**x**	
Any other information that may be offensive to colleagues, breaches the integrity of the ethos of the school, or brings the school into disrepute				**x**	
Other activities					
Using school systems to run a private business				**x**	
Using systems, applications, websites, VPNs, proxies or other mechanisms that bypass filtering or other safeguards employed by the school				**x**	
Infringing copyright, including by passing off AI-generated work as one's own where this is not permitted				**x**	
Revealing or publicising confidential or proprietary information, e.g. financial or personal information, databases, network				**x**	

access codes and passwords					
Entering personal, sensitive or special category data into a generative AI tool				x	
Creating or propagating computer viruses or other harmful files				x	
Unfair usage — downloading or uploading large files that hinder others in their use of the internet				x	
Online gaming (educational)			x		
Online gaming (non-educational)				x	
Online gambling				x	
Online shopping and commerce			x		
File sharing				x	
Use of social media			x		
Use of messaging apps		x			
Use of video broadcasting, e.g. YouTube		x			
Use of generative AI tools not on the school's approved list				x	

18. Responding to incidents, actions and sanctions

This guidance is for use when staff need to manage incidents involving the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see Section 17).

Illegal incidents

If there is any suspicion that the website or websites concerned may contain child sexual abuse images, or if there is any other suspected illegal activity, follow the right-hand side of the flow chart at Appendix 3 and report immediately to the police. Do not attempt to investigate further.

Procedure where misuse is suspected

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in the process. This is vital to protect individuals if accusations are subsequently made.
- Conduct the procedure using a designated computer that will not be used by young people and that can, if necessary, be taken off site by the police. Use the same computer for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, and that the sites and content visited are closely monitored and recorded for their protection.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for the investigation. These may be printed, signed and attached to the record — except in the case of images of child sexual abuse.
- Isolate the computer in question as far as possible. Any change to its state may hinder a later police investigation.

Once this has been completed and fully investigated, those involved will need to judge whether the concern has substance. If it does, appropriate action will be required and could include:

- Internal response or discipline procedures
- Involvement by the local authority or a national or local organisation, as relevant
- Police involvement or action

If the content being reviewed includes images of child abuse, monitoring must be halted and the matter referred to the police immediately. Other instances to report to the police include:

- Incidents of grooming behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act 1959
- Criminally racist or terrorist material
- Other criminal conduct, activity or materials

It is important that all of the above steps are taken, as they provide an evidence trail for the school and possibly the police, and demonstrate that visits to these sites were carried out for child protection purposes. The completed record should be retained for evidence and reference purposes.

Actions and sanctions — students

It is more likely that the school will need to deal with incidents involving inappropriate rather than illegal misuse. It is important that incidents are dealt with as soon as possible, in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. Incidents of

misuse will be dealt with through normal behaviour and disciplinary procedures, taking account of the student's age, understanding and any special educational need or vulnerability. Where an incident indicates that a child may be at risk of harm, the safeguarding response takes precedence over the behaviour response.

Student incidents — all incidents will be thoroughly investigated and any of the following may apply, depending on mitigating factors	**Refer to class teacher / tutor**	**Refer to phase or department lead**	**Refer to head teacher**	**Refer to DSL**	**Refer to police**	**Refer to technical support re filtering / security**	**Inform parents / carers**	**Removal of network / internet access rights**	**Warning or further sanction**
Deliberately accessing or trying to access material that could be considered illegal		x	x	x	x	x	x		x
Unauthorised use of non-educational sites during lessons	x								
Unauthorised use of a mobile phone, smart watch, digital camera or other personal device	x	x	x				x		x
Unauthorised use of social media, messaging apps or personal email	x	x	x				x		
Unauthorised downloading or uploading of files	x	x	x					x	
Allowing others to access the school network by sharing username and password	x	x	x			x			x
Attempting to access, or accessing, the school network using another student's account	x	x	x			x			
Attempting to access, or accessing, the school network using a member of staff's account	x	x	x			x	x	x	x
Corrupting or destroying the data of other users	x	x	x				x	x	x
Sending an email, text or message that is offensive, harassing or of a bullying nature	x	x	x	x			x	x	

Creating, requesting or sharing a nude, semi-nude, sexual or AI-generated intimate image of another person			x	x	x		x		x
Using AI tools to create abusive, discriminatory or harassing content about another person		x	x	x			x		x
Using proxy sites, VPNs or other means to subvert the school's filtering system	x	x	x			x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x			x	x		x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x		x	x	x	x
Receipt or transmission of material that infringes copyright or data protection law	x	x	x						x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x				x		x
Continued infringements of the above, following previous warnings or sanctions	x	x	x				x	x	x

Actions and sanctions — staff and volunteers

Where a concern relates to a member of staff, the trust's Managing Allegations and Concerns policy applies, and concerns that meet the harm threshold are referred to the Local Authority Designated Officer. Low-level concerns are recorded and reviewed in line with Part Four of Keeping Children Safe in Education.

Staff and volunteer incidents	Refer to line manager	Refer to head teacher	Refer to DSL	Refer to LADO / police	Refer to technical support re filtering / security	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		x	x	x	x	x

Excessive or inappropriate personal use of the internet or school systems in school time	x	x				x
Unauthorised downloading or uploading of files	x	x			x	
Allowing others to access school systems by sharing username and password, or attempting to access another user's account	x	x			x	x
Careless use of personal data, or a personal data breach	x	x				x
Sending an email, text or message that is offensive, harassing or of a bullying nature	x	x	x			x
Using personal email, social media or a personal device to communicate with students or parents	x	x	x			x
Photographing or recording students on a personal device	x	x	x			x
Entering personal or special category data into a generative AI tool, or using an unapproved AI tool with student data	x	x				x
Actions which could compromise the member of staff's professional standing, or bring the school into disrepute	x	x	x			x
Using proxy sites or other means to subvert the school's filtering system	x	x			x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x		x
Breaching copyright or licensing regulations	x	x				x
Continued infringements of the above, following previous warnings or sanctions	x	x				x

19. Recording, monitoring and reviewing this policy

Recording incidents

- All online safety concerns are recorded on the school's safeguarding recording system, and behaviour-related incidents on the behaviour system, with a clear link where both apply.
- Records include the date, the students or staff involved, what happened, the action taken, who was informed, and the outcome.
- An online safety incident log (Appendix 4) is maintained by the DSL to allow trend analysis across the school.
- Records are retained in line with the trust's retention schedule.

Reporting

- The DSL reports online safety incident trends, filtering and monitoring assurance, and training completion to the headteacher each term and to governors at least termly.
- The Online Safety Governor reports to the full governing body, and the trust receives an annual report.
- Significant incidents are reported to the trust safeguarding lead without delay.

Annual review and risk assessment

Keeping Children Safe in Education states that schools and colleges should carry out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. In addition, the effectiveness of filtering and monitoring must be reviewed at least once every academic year.

- The annual review and risk assessment are led by the DSL, involve the safeguarding team and the IT Lead, and draw on incident data, student voice, staff feedback, monitoring reports and the audit tools at Appendix 2.
- The outcome is a written action plan with named owners and dates, signed off by the headteacher and the Online Safety Governor.
- This policy is reviewed annually, or sooner if there is a significant change in technology, statutory guidance or the school's risk profile, and is approved by governors.

> *An online safety audit should be neither a tick-box exercise nor a static report: it should be a living document that reflects the fluid realities of technological change, evolving harms and user behaviours.*

20. Related policies, legislation and national resources

Related school and trust policies

- Child Protection and Safeguarding Policy
- Behaviour Management / Positive Relationships Policy (including mobile phone arrangements)
- Anti-Bullying Policy
- Embark Trust Acceptable Use of the Internet and Electronic Communication
- Staff Code of Conduct
- Managing Allegations and Concerns Policy
- Data Protection Policy and retention schedule
- Confidentiality Policy
- Complaints Policy
- Remote Learning Policy
- Whistleblowing Policy
- Cyber incident response and business continuity plan

Legislation

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011, Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Children Act 1989
- Protection of Children Act 1978
- Criminal Justice Act 1988, section 160
- Computer Misuse Act 1990
- Obscene Publications Act 1959
- Human Rights Act 1998
- Health and Safety at Work etc. Act 1974
- Equality Act 2010
- Voyeurism (Offences) Act 2019
- Online Safety Act 2023
- Children's Wellbeing and Schools Act 2026

Guidance

- Keeping children safe in education
- Mobile phones in schools
- Filtering and monitoring standards for schools and colleges
- Meeting digital and technology standards in schools and colleges
- Generative artificial intelligence (AI) in education
- Generative AI: product safety expectations
- Teaching online safety in schools

- Searching, screening and confiscation
- Harmful online challenges and online hoaxes
- Sharing nudes and semi-nudes: advice for education settings
- NCSC cyber security guidance for schools
- NEN technical guidance
- DDSCP — Online Safety and Internet Abuse procedures

National links and resources

- Thinkuknow (CEOP education)
- CEOP Safety Centre — report abuse
- Childnet
- Internet Matters
- Internet Watch Foundation
- Report Remove (Childline and IWF)
- Lucy Faithfull Foundation
- NSPCC online safety
- Childline
- The Marie Collins Foundation
- UK Safer Internet Centre
- Professional Online Safety Helpline
- SWGfL 360 Safe self-review tool
- LGfL online safety audit
- Cyber Choices (National Crime Agency)
- Action Fraud

Appendix 1: Student Acceptable Use Agreement templates

Schools should adapt these templates to their phase and context. Agreements should be revisited at the start of each academic year and explained in an age-appropriate way, rather than simply signed.

Version A — Early Years and Key Stage 1

These rules help us to stay safe when we are using computers, tablets and the internet.

- I will only use the computers and tablets when a grown-up says I can.
- I will only visit the websites and apps that my teacher has chosen.
- I will ask a grown-up before I click on something new.
- I will be kind when I write or send messages.
- I will not share my password with anyone except my teacher or my grown-up at home.
- I will not tell people I meet online my name, where I live or where I go to school.
- I will not take photos or videos of other people unless my teacher says I can.
- If something makes me feel worried, upset or unsure, I will tell a grown-up straight away.
- I know a computer can sometimes get things wrong, and that I should check with a grown-up.
- I know that if I break these rules, I might not be able to use the computers for a while.

Name of student		**Class**	
Signed (student)		**Date**	
As the parent or carer of the above child, I give permission for my child to have access to the internet and ICT systems at school, and I have talked through these rules with them.			
Signed (parent / carer)		**Date**	

Version B — Key Stage 2 and above

This agreement helps to keep me safe and to make sure that everyone can use technology fairly and responsibly.

Using school technology

- I will only use school devices, accounts and systems for schoolwork, and only when I have permission.
- I will keep my username and password private, and I will not use anyone else's account or let anyone use mine.
- I will not try to get around the school's filtering or security systems.
- I will not download or install software on school devices.
- I understand that my use of school devices, accounts and the school network is monitored.

Behaviour online

- I will treat other people with respect online, and I will not send or share anything that is unkind, threatening, discriminatory or embarrassing to someone else.
- I will not take, share or post photos or videos of other people without their permission.
- I will not share personal information about myself or anyone else online.
- I understand that the school's rules also apply to things I do online outside school where they affect other members of the school community.

Mobile phones and personal devices

- I understand that I must not have access to my mobile phone, smart watch or similar device during the school day, including at break and lunchtime, unless the headteacher has agreed an exception for me.
- I understand that staff may confiscate a device if this rule is broken.

Artificial intelligence

- I will only use AI tools that my school has approved, and only when a teacher has said I can.
- I will not type personal information about myself or anyone else into an AI tool.
- I understand that AI can be wrong, biased or made up, and I will check anything important.
- I will be honest about when I have used AI in my work, and I understand that passing off AI work as my own is not allowed.
- I understand that using AI to create nude, sexual or humiliating images of anyone is extremely serious, may be a criminal offence, and will be dealt with as a safeguarding matter.

Getting help

- If I see something online that upsets, worries or confuses me, I will tell a member of staff or a trusted adult straight away.
- If someone asks me for pictures of myself, threatens me, or asks me to keep a secret, I will tell an adult — I know I will not be in trouble.
- I know how to report a concern in school, and I know I can also use the CEOP report button, Childline and Report Remove.
- I understand that if I break this agreement, my access to devices and the internet may be restricted, my parents or carers may be informed, and further sanctions may apply.

Agreement — Key Stage 2 and above

Name of student		**Class**	
Signed (student)		**Date**	
As the parent or carer of the above child, I give permission for my child to have access to the internet and ICT systems at school. I have read and discussed this agreement with them, and I understand the school's expectations on mobile phones and the use of AI tools.			
Signed (parent / carer)		**Date**	

Appendix 2: Annual online safety audit and risk assessment tools

Keeping Children Safe in Education states that schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. The 2026 edition additionally requires that the effectiveness of filtering and monitoring is reviewed at least once every academic year, and that the school can demonstrate this has taken place.

It is vital that an online safety audit is neither treated as a tick-box exercise, nor viewed as a static report: it should be a living document that reflects the fluid realities of technological change, evolving harms and user behaviours.

An online safety audit should be carried out by, or with, the safeguarding team, in recognition that the designated safeguarding lead should take lead responsibility for safeguarding and child protection, including online safety.

Free self-review tools

- Online Safety Self-Review Tool for Schools — 360safe
- Online Safety Audit — LGfL
- UK Safer Internet Centre — filtering and monitoring testing tools

Governance tools

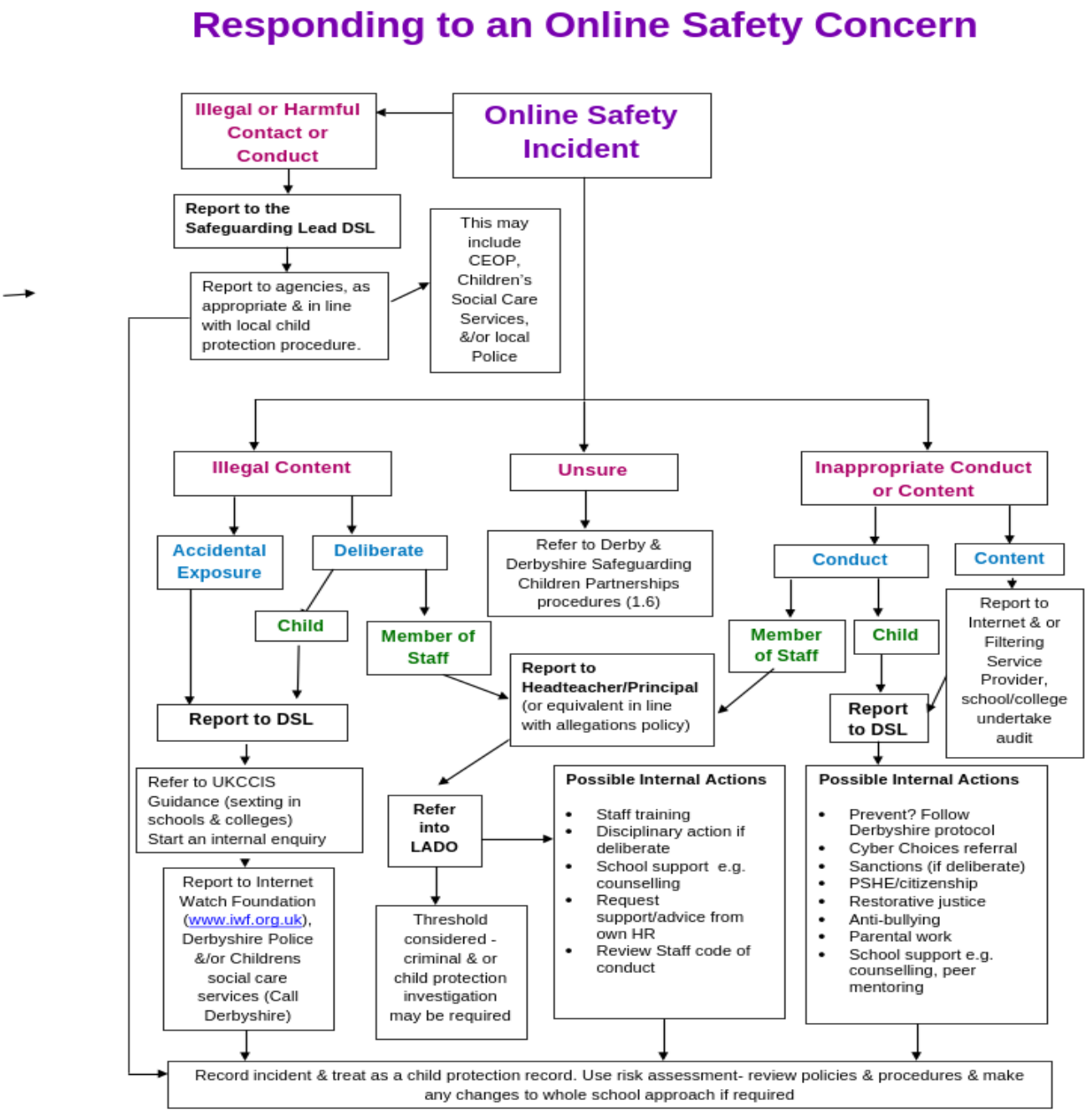
UKCIS has published Online safety in schools and colleges: questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping children safe online, to learn how to improve that approach where appropriate, and to find out about tools which can be used to improve it.

UKCIS has also published an Online Safety Audit for ECTs and ITTs, which helps mentors of trainee teachers and early career teachers induct mentees and provide ongoing support, development and monitoring.

Minimum evidence to retain each year

- The completed online safety risk assessment, dated and signed off
- The record of the filtering and monitoring effectiveness review, including who led it, what was tested and what was found
- The resulting action plan, with owners and completion dates
- Filtering change control logs and a sample of monitoring alert responses
- Training completion records for staff, governors and trustees
- Incident log trend analysis and the report to governors
- The approved AI tools register and associated DPIAs

Appendix 3: Responding to an online safety concern — flow chart



Appendix 4: Online safety incident log template

Maintained by the DSL. Used alongside, not instead of, the school's safeguarding recording system, to allow trend analysis and reporting to governors.

Date and time	Reported by	Students / staff involved	Nature of incident (4Cs category)	Action taken and by whom	Outcome / referral / review date

Prompts for the record: Was a parent or carer informed? Was the DSL informed, and when? Was a referral made to children's social care, the police or another agency? Was the trust safeguarding lead informed? Did the incident indicate a gap in filtering, monitoring, curriculum or training — and what has changed as a result?

Appendix 5: AI tool approval checklist

To be completed by the requesting member of staff and reviewed by the IT Lead and DSL before any generative AI tool is used with students or with school data. Retain with the DPIA.

#	Check	Evidence / notes
1	What is the educational purpose, and is there an existing approved tool that already meets it?	
2	Who will use it — staff only, or students? If students, what is the provider's minimum age, and does it match our cohort?	
3	Does the tool process personal data? If so, has a DPIA been completed and logged with the trust DPO?	
4	Where is data stored and processed, is it used to train the provider's models, and can that be turned off?	
5	Has the product been assessed against the DfE's Generative AI: product safety expectations?	
6	What content safety measures does the provider apply, and can outputs be filtered or restricted for education use?	
7	Can our filtering and monitoring see and log interactions with this tool? If not, what mitigations are in place?	
8	What is the process if a student is exposed to harmful content, or discloses something concerning, through the tool?	
9	Does the tool include chatbot, companion or persona features that could create a contact risk?	
10	What are the intellectual property and accessibility implications?	
11	What training will staff need, and what will students be taught before use?	
12	How will use be reviewed, and when will approval be reconsidered?	

Requested by		**Date**	
Approved by (IT Lead)		**Date**	
Approved by (DSL)		**Review date**	