Gatley Primary School

Online Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Version: 1

Date created: September 2026

Next review date: September 2027

Scope of the Online Safety Policy

This Online Safety Policy sets out how Gatley Primary School will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, Gatley Primary School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Policy development, monitoring and review

This policy has been developed by the Online Safety Group drawing on the expertise and responsibilities across the school. Membership includes:

- Headteacher / Senior leaders
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL)
- Staff (including teaching, support and technical staff)
- Governors
- Parents/carers

Consultation with the wider school community has taken place through a range of formal and informal opportunities to ensure the policy is understood, workable and proportionate.

Schedule for approval, monitoring and review

Approved by the Governing Body on: 4/11/26

Monitored by: *SLT*

Monitoring frequency: *Annually*

Reporting to the Governing Body: *Annually*

Policy review cycle: reviewed annually, or sooner in response to significant technological developments, emerging risks, or incidents.

Next planned review date: September 2027

Escalation following serious incidents: the school will inform relevant external agencies as appropriate, e.g., *Trust, the Local Authority safeguarding lead, and/or the police*.

Monitoring the impact of the policy

The school will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Learners, Parents/carers, Staff

Policy and leadership

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded

Governors approve the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated
- Ensure that children be taught about safeguarding, including in relation to online safety
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

Governors

The governing body will nominate safeguarding Governor who will:

- Meet regularly with the DSL/OSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).

- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the relevant governor group/committee:
- Undertake basic cyber security awareness training and support school cyber security oversight.

Governors also support parent/carer and community engagement in online safety.

Designated Safeguarding Lead (DSL)

KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to explicit in the DSL's job description.

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information
- With the nominated SLT Lead and the IT provider lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for learners with SEND.

Online Safety Lead (OSL)

The OSL will:

- Lead the Online Safety Group and support the DSL day to day.
- Lead development and review of online safety documentation.

- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Curriculum Leads

Curriculum leads will work with the DSL/OSL to deliver a planned online safety programme (e.g. ProjectEVOLVE) through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider / technical staff

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.

- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to the headteacher
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Learners

Learners will:

- Follow the Learner AUA and Online Safety Policy
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly in line with the AUA
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy and share the learner AUA
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

Online Safety Group-

The Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice.

Membership

- DSL, DDSL, Senior Leader(s)
- Staff representatives (STEAM curriculum team)
- Learner representative- Department for Digital Culture

Core responsibilities

The group supports the DSL/DDSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Gather feedback from learners, staff and parents/carers and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.
- Track and evidence improvement actions (e.g. 360 safe).

Governance and impact

- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Learner Voice as needed.
- Reports key themes, actions and impact to SLT and governors, and shares appropriate summaries with the wider community.

Policy

Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding/Child Protection, Behaviour, Anti-Bullying and Data Protection policies.

What the policy does

- Defines responsibilities for online safety.
- Sets expectations for safe, professional and ethical use of technology (including AI).
- Sets out reporting, recording and response procedures for online safety incidents.

- Supports compliance with KCSIE, DfE Technical Standards and UK GDPR.
- Promotes learners' digital competence and critical understanding.

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually, and sooner if risks/technology change.
- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. 360 safe, ProjectEVOLVE).
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training.
- Communicated to learners and parents/carers through AUAs and awareness activity.
- Published on the school website.

Acceptable use

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs). AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

- staff and learner induction/handbooks
- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- school website
- peer support / learner-led activity

Reporting and responding

Introduction

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The school recognises national findings, including the *Ofsted Review of Sexual Abuse in Schools and Colleges (2021),* which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns.

Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools (e.g., Whisper), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):

    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring

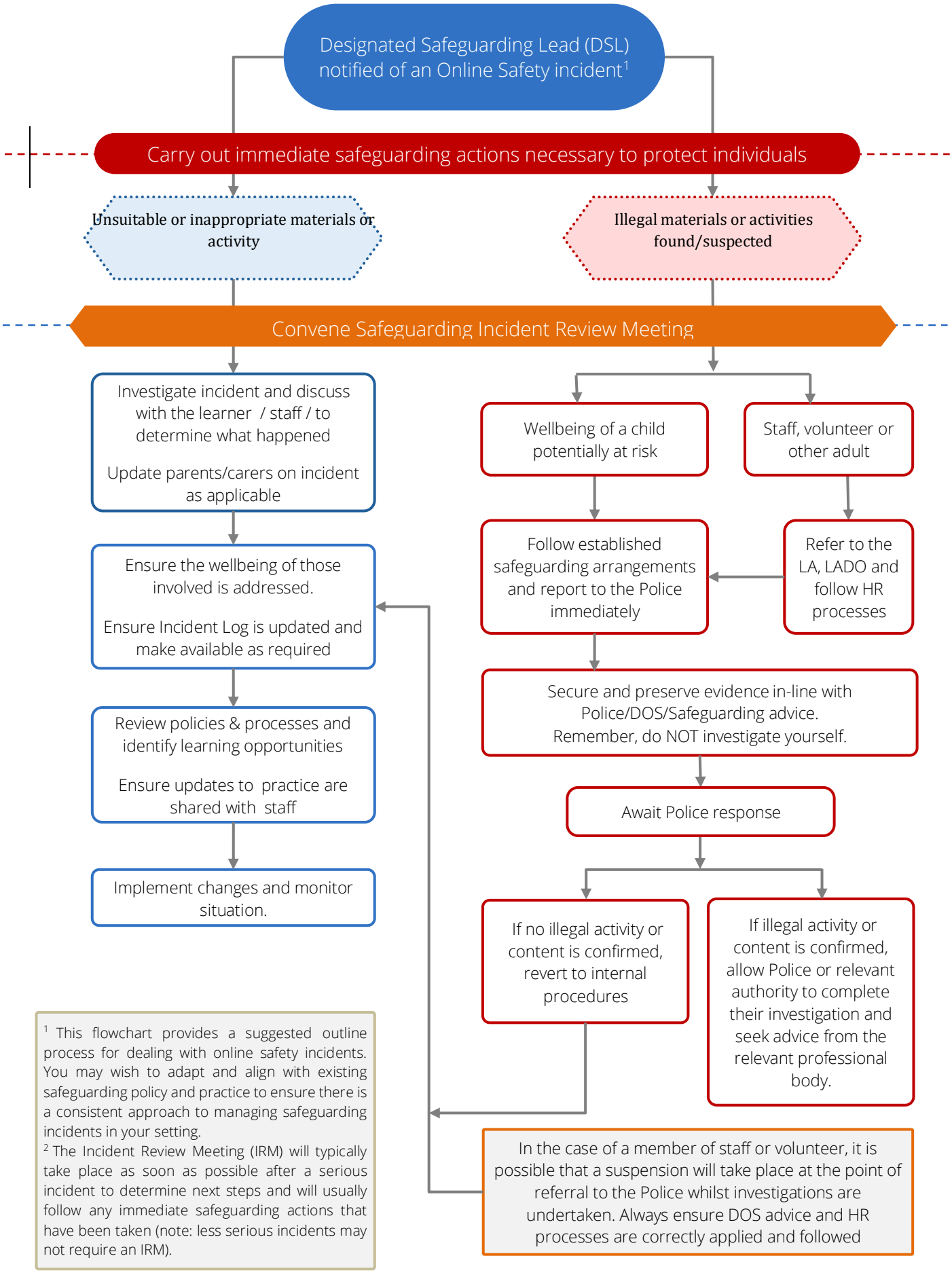
The school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
    - The Online Safety Group
    - Senior leaders
    - Governors (via safeguarding reports)
    - *Staff*
    - *Learners, where appropriate*
    - *Parents/carers through general communications*
    - *Local safeguarding partners where relevant*

External Support and Escalation

The school will work with appropriate external agencies when required, including:

- Local Authority safeguarding teams
- Local Authority Designated Officer (LADO)
- Police / CEOP
- Local Safeguarding Partnership guidance (e.g., harmful sexual behaviour support)
- *UK Safer Internet Centre's Professionals Online Safety Helpline*
- *Reporting Harmful Content service*



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any 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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

AI must only be used in line with the AUA.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

Policy statements

The school will:

- Implement the Acceptable Use Agreement with regards to AI
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used in line with the AUA, staff should use anonymised data only.
- Require UK GDPR compliance. In line with the AUA, staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to a DSL/SLT.

- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support learners in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

Education

Online Safety Education Programme

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including DfE "Teaching Online Safety in Schools", UKCIS "Education for a Connected World", and resources such as SWGfL ProjectEVOLVE). Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, Health Education, Computing and Citizenship), with assessment and clear intended outcomes.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;

- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation and opportunities such as Pupil Parliament – Department for Digital Culture, campaigns, and contribution to acceptable use and community-facing online safety activities. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Staff

In line with DfE Keeping Children Safe in Education (KCSIE), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include:
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement
- staff are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles
- staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for learners are approved and managed.
- staff follow cyber security policy and requirements.
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources (e.g. ProjectEVOLVE EDU) and, where appropriate, enhanced pathways (e.g. ProjectEVOLVE SAFEGUARDING).
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/DDSL (or nominated staff) to individuals as required.

Governors

Governors should take part in online safety training and awareness activity. This is particularly important for governors serving on committees with responsibility for safeguarding, online safety, technology or health and safety.

Training and updates may be provided through :

- Attendance at training offered by the Local Authority, MAT or other relevant organisations (e.g. SWGfL).
- Participation in school training and information sessions (for example, staff briefings or parent events). This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

Enhanced training will be provided for (at least) the Safeguarding Governor. This will include:

- Basic cyber security awareness training.
- Training to understand the school's filtering and monitoring provision, enabling effective participation in required checks and reviews.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

Working with Parents and Carers

The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.

- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources (e.g. UK Safer Internet Centre, Internet Matters, Childnet, SWGfL).
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches
- accurate, balanced and age-appropriate information about changes affecting social media and other online services
- guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

The school recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.

- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice, including through recommended tools such as 360 Early Years or 360 Groups.

Technology

Purpose

The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider school community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Detailed arrangements are set out in the Appendix C1 - Filtering and Monitoring Policy Template and Appendix C2 - Technical Security Policy Template.

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., DfE Technical Standards, KCSIE) and best practice guidance (e.g., UKSIC Appropriate Filtering and Monitoring)

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated

- Where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Securly). Reviews will be carried out by the SLT, with the support of the school's designated safeguarding lead. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement

- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. (KCSIE 2026 refers to the DfE Cyber Security Standards and recognises cyber security as a safeguarding issue).

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and their safeguarding implications and receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation. (The Data (Use and Access) Act 2025 makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards)

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests

- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration.
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.
-

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

Technology Practice

Purpose

The school recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in Keeping Children Safe in Education, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice, education. and staff training. It also supports the DfE digital and technology standards and the school's responsibilities for filtering, monitoring, cyber security and digital leadership.

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated with the AUP
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education
- learners do not have access to mobile phones or other personal smart devices throughout the school day.
- any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or SEND-related reasons
- staff model the school's requirements and use personal devices only where authorised and professionally appropriate

Decisions about device use are informed by risk assessment and reviewed regularly.

Digital Content

The school recognises that multi-modal digital content (inc. AI) can enrich learning and communication when used responsibly. Its approach supports safeguarding requirements in particular, sexual imagery, consent, coercion, privacy and the sharing or manipulation of content.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully

- school-approved platforms and accounts are used where content includes personal or sensitive information
- staff and learners understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on Protecting your setting's images from AI manipulation and abuse

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (guidance is available from UKSIC)
- publishing public communications is restricted to authorised and trained staff
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour

- the school communicates confirmed changes to policy in line with best practice and Government guidance.

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, learners and parents
- national guidance and statutory expectations
- the school's progress towards meeting the DfE digital and technology standards
- the impact of mobile-phone arrangements and changes affecting children's access to online services.

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, learners and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes. Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety

Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about the Cyber Choices programme. Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.

- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to

imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic

form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices for DfE guidance)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

https://www.gov.uk/guidance/what-academies-free-schools-and-colleges-should-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Online Safety Act 2023

The Online Safety Act 2023 is a new set of laws that protects children and adults online. It puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms. The Act will give providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

Ofcom is the independent regulator of Online Safety. It will set out steps providers can take to fulfil their safety duties in codes of practice. It has a broad range of powers to assess and enforce providers' compliance with the framework.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools / Resources for Schools / other organisations

Whisper Anonymous Reporting Tool - https://swgfl.org.uk/products/whisper/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
SWGfL Test filtering - http://testfiltering.com/
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations
Childline – Report / Remove
SWGfL- Assisted Monitoring
SWGfL – Resources for Education
DfE Using AI in education settings: support materials

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

SWGfL - ProjectEvolveEdu

UKCCIS – Education for a connected world framework

Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/

Data Protection

DfE – Data Protection in schools toolkit

ICO Guides for Organisations

ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

UK Safer Internet Centre Professionals Online Safety Helpline

SWGfL – Online Safety Training

Infrastructure/Technical Support/Cyber-security

DfE – Technical Standards for Schools and Colleges

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

SWGfL - Cyber Security in Schools.

NCA – Guide to the Computer Misuse Act

SWGfL- Assisted Monitoring

Secure Schools – Cyber Security

Working with parents and carers

Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Childnet – Trust Me

Research

Ofcom – Childrens Media Habits
Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in April 2026. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2026

Appendix 1:

ICT Acceptable Use Agreement 2026/27

For Staff, Governors/Trustees and Volunteers

To ensure that members of staff, governors and volunteers are fully aware of their professional responsibilities when using information systems and when communicating, you are asked to read and sign this ICT Acceptable Use Agreement. You must also familiarise yourself with the ELT Code of Conduct and Child Protection & Safeguarding policies for further information and clarification.

The Agreement:

- I understand that ICT includes a wide range of systems and agree to not use any ICT devices, emails, or networking sites in the Trust/School setting for activities which would contravene the values of the Trust/School and professional conduct.
- I understand that the Trust/School's digital technology resources and systems must not be used for personal or private business unless explicitly authorised and their use is compliant with data protection policies.
- I understand that the use of my own (personal) device in Trust/School is only permitted in designated areas with the express permission of the Headteacher/Principal/CEO (or their delegated representative).
- I will ensure that any ICT equipment is stored safely.
- I will always use a laptop bag when transporting a school/trust laptop.
- I understand that I may be asked to cover the cost of repairs to equipment/laptops allocated to me where damage falls outside of the scope of normal wear and tear.
- When I take ICT equipment off site, I will ensure the integrity of data and information

including keeping equipment safe and equipment will not be left unattended when off site.

- I will ensure that I log off or lock the screen when leaving a device unattended.
- I understand that the Trust/School digital technology resources and the content held within its information systems may not be used for personal purposes.
- I will not download or install any software or hardware without permission of an authorised Trust/School representative (with responsibility for system / network management).
- I will not disclose my password/login credentials and will follow 'good practice' advice in the creation and use of my password. If I feel my password has been compromised, I will contact the ICT staff responsible for the network immediately.

- I will not allow unauthorised individuals to access email, internet, or any Trust/School network or system that I have access to.
- I will ensure any documents containing sensitive information are password protected
  before emailing and will share the password securely with the recipient.

- I will only take and store photographs or videos of students using Trust/School approved devices.
- I will only save photographs and videos of students and staff securely within the Trust/School network and use/share appropriately with permission.
- I will not use open AI platforms.
- I will only access closed AI platforms with prior agreement from the Headteacher/Principal/CEO.
- I will not process school, personal or sensitive data via AI platforms.
- I will respect copyright and intellectual property rights.
- I will ensure that all my electronic communication including emails and instant messaging are in keeping with my professional role.

- I will only access Trust/School resources remotely using the Trust/School ICT contractor approved system and follow e-security protocols to interact with them.
- I am aware of the rules for computer and internet usage for students and will promote e- safety with students in my care.
- I will use appropriate search engines and websites when working with students and will supervise students using the internet during lessons.
- I will report any faults, malfunctions or suspected viruses, including those that may be attached to emails, to the contracted ICT support staff, including full details and all error messages immediately.
- I will not store any sensitive personal or special category data containing personal and special category data on any unencrypted media, on local non-networked drives or non-sanctioned cloud storage.
- I will ensure all documents, data etc. are printed, saved, accessed, retained, and deleted in accordance with UK GDPR, DUAA and internal data retention policies.
- I will not use a personal email address for School, Trust or Governance communications and will only use my School or Trust issued email address.
- I will report any breach of this agreement to the Headteacher/Principal/CEO, or a member of the Senior Leadership Team in their absence.
- I understand that Trust digital technology resources must not be used for personal commercial activities, private business interests or any use that conflicts with Trust business. Limited incidental personal use may be permitted in accordance with the ICT Acceptable Use Policy

The Trust/School may exercise its right to monitor and audit the use of the Trust/School's information systems, devices and Internet access, for policy compliance and to intercept emails and to delete inappropriate materials where it believes unauthorised use of the

Trust/School's information system or content may be taking place; or that the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Declaration:

- I have read, understood and accepted the ICT ACCEPTABLE USE AGREEMENT.
- I agree to abide by all the statements within.
- I understand that I have a responsibility for myself and others' e-safeguarding.
- I undertake to be a safe and responsible digital technologies user.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the Trust/School's most recent policies including the Child Protection & Safeguarding and Code of Conduct.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Name	
Signature	
Date	