



St. Paul's School Online Safety Policy



Approving Body:	FGB
Date of Adoption:	September 2026
Date of Review:	September 2027

Please read in conjunction with the following:

Safeguarding Policy
Staff Behaviour Policy
Behaviour Policy
Acceptable Use Agreements
PSHE Curriculum

Contents:

- 1. Vision and Values**
- 2. Responsibilities**
- 3. Use of Artificial Intelligence (AI) in Schools**
- 4. Online Safety Education Programme**
- 5. Filtering and Monitoring**
- 6. Technical Security**
- 7. Public Online Communications**
- 8. Review**

1. Vision and Values

St Paul's Primary School's Online Safety Policy sets out how we use digital tools in ways that reflect our values of kindness, creativity and pride, alongside our Ready, Respectful, Safe expectations. These values guide how every member of our community, children, staff and families, behaves both offline and online, ensuring that the way we communicate, collaborate and participate in digital spaces mirrors the warmth, care and high standards of our school. We celebrate the opportunities technology provides and use it widely to support imaginative learning and innovative practice, while recognising that its benefits rely on everyone acting kindly, respectfully and safely whenever they engage online. Through this shared commitment, we create a digital culture where creativity thrives, relationships are protected and every member of St Paul's feels confident, safe and proud of the way they represent themselves and our school.

This Online Safety Policy sets out how St. Paul's 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 and visitors. 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, we 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.

2. 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.

The Headteacher and 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, 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.
- Ensure an annual review of the effectiveness on filtering and monitoring systems and ensure that these are recorded

Governors will:

- 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.

The governing body will nominate a Safeguarding Governor who will:

- Meet regularly with the DSL.
- Receive anonymised incident and monitoring summaries, including safeguarding concerns linked to digital safety.
- 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 full governing board.
- Undertake basic cyber security awareness training and support school cyber security oversight.

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 and IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- At least annually and with the support of the IT provider, complete a review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.
- Ensure appropriate support for learners with SEND.

Curriculum Leads will:

- Work with the DSL to deliver a planned online safety programme (e.g. Project EVOLVE) through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.
- Take responsibility for assemblies related to online safety.
- Ensure that the Acceptable Use Policy is distributed annually to new starters and when updates are made.

Teaching and Support Staff will:

- Uphold professional standards online and contribute to a strong safeguarding culture.
- Follow the Online Safety Policy, Safeguarding Policy, Behaviour Policy and sign/comply with the Staff Acceptable Use Agreement.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues.
- Embed online safety where appropriate.
- 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.

The IT provider will:

- Support leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.
- 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 the DSL.
- Monitor systems for misuse and report concerns promptly to the DSL.
- Follow the school's Online Safety policy and keep technical knowledge current.

Learners will:

- Follow the Acceptable Use Policy, Online Safety Policy and Behaviour Policy.
- Report concerns and know how to get help.
- Use technology responsibly, respecting others.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers will:

- Be key partners in reinforcing safe online behaviour.
- Support pupils to understand and sign the acceptable use policy.
- Read and sign the acceptable use policy.
- Report concerns to the DSL if they have them.

The school will:

- Publish the Online Safety Policy and Acceptable Use Agreements on the school website.
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, emails, messages and the school website, as appropriate.

3. Use of Artificial Intelligence (AI) in Schools

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.

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

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by 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, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- 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 the DSL and where appropriate record any GDPR breaches related to the use of AI.

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.

4. 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 parts of 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 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 such as PSHE. The curriculum structure is published on the school website.

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 approval from the DSL and a robust and clear rationale- but this is as a last resort and when no other unfiltered platform is appropriate for the activity.

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.

In addition to providing a robust curriculum for pupils in school, we will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website and digital communication tools.
- Involving learners in sharing online safety messages with parents/carers
- Signposting parents and carers to trusted national resources (e.g. NSPCC, Report Remove, CEOP) as part of our Early Help website page.
- 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, authorised exceptions and the consequences of breaches, as part of our school Behaviour Policy
- 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

5. 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](#), DfE [Generative AI: product safety standards](#); [KCSIE](#)). The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

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
- 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), IT staff and governors have clear roles and responsibilities
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- Filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using [Testfiltering](#)). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. 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.

6. 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:

- Senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance
- Staff receive regular cyber-security training covering phishing, credential theft, malicious links, social engineering, ransomware, AI-enabled scams and other emerging threats.
- Learners receive age-appropriate education about cyber security, scams, account protection and the lawful and responsible use of systems.
- Learners receive age-appropriate education on cyber risks
- Governors understand their oversight responsibilities
- 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 including [The Data \(Use and Access\) Act 2025](#).

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.

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.
- Device use is consistent with safeguarding, behaviour and acceptable use policies.
- 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, in accordance with the school's Behaviour Policy and in line with the [DfE statutory guidance](#).
- Any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical related reasons
- Staff model the school's requirements and use personal devices only where authorised and professionally appropriate.
- Procedures laid out in the Behaviour Policy cover possession, storage, confiscation and return of devices, in accordance current national guidance.

7. 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.
- 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.
- Staff understand expectations around professional conduct and online behaviour.
- The school communicates confirmed changes to policy in line with best practice and Government guidance.

8. Review

A formal review of the policy will take place biannually or in line with any significant changes.

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 impact of mobile-phone arrangements and changes affecting children's access to online services