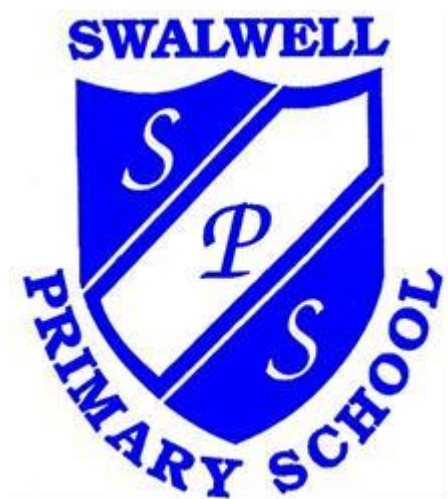


Swalwell Online Safety Policy



Academic year	Head teacher	Head of School	School Business Manager	Chair of Governors
26/27	Mrs R Hocking	Miss G Jelly	Mrs E Elliott	Mrs L Gray

Review Date	Changes made	By whom	Date Shared
March 2020	Yes	AHT KM	March 2020
December 2020	Yes	KM RT	December 2020
September 2022	NO		September 22
March 26	Yes	KMcC	March 26

Introduction

1. Introduction & Purpose

This policy sets out how Swalwell Primary School safeguards pupils online and promotes safe, responsible and positive use of digital technologies at school and at home. It reflects the statutory requirements in *Keeping Children Safe in Education (KCSIE) 2025* and relevant Department for Education (DfE) standards on filtering and monitoring, and should be read alongside our *Child Protection, Safeguarding, Behaviour/Anti-Bullying and Data Protection policies*.

Rationale:

The potential that technology has to impact on the lives of all people increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than adults. In many areas, technology is transforming both the way schools teach and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. These trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use, which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we help those who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

2. Scope & Audience

This policy applies to all pupils, staff, governors, trainees, volunteers, visitors, contractors, and any other users of the school's network, devices and online services. It also sets expectations for parents/carers to support safe online behaviours at home.

3. Legal & Statutory Framework

- Keeping Children Safe in Education (KCSIE) 2025 (statutory) — including strengthened online safety expectations and the 4Cs risk framework (content, contact, conduct, commerce).
- DfE Digital & Technology Standards: Filtering and Monitoring (core standard; updated guidance and leadership responsibilities).
- DfE 'Plan Technology for Your School' self-assessment service (to review filtering/monitoring and wider digital standards).
- Education for a Connected World framework (to underpin curriculum progression).
- Data Protection Act 2018 / UK GDPR, and school data protection policies.

The Law

This policy has been drawn up based on legislation, policy and guidance that seeks to protect children in England.

Our Online Safety Policy has been written by the school, using advice from Gateshead LA, and government guidance. The Policy is part of the School's Improvement Plan.

Plan and related to other policies including Positive Learning, Safeguarding and Data Protection policies.

As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up-to-date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

Roles and Responsibilities

All at Swalwell Primary are committed to safeguarding children in our care. This policy has been developed by the Online Safety / Computing Lead and the Senior Leadership Team in order to ensure that it truly reflects our robust and thorough approach to safeguarding. This section outlines responsibilities of staff, leaders and stakeholders as well as all users of technology within school.

Role	Key Responsibilities
Head Teacher	• Overall accountability for online safety, including oversight of filtering and monitoring and ensuring compliance with KCSIE and DfE standards. • Ensures appropriate training and resources are in place, and that safeguarding responses are timely and effective.

Designated Safeguarding Lead (DSL) / Online Safety Lead	• Day-to-day leadership of online safety, policy maintenance, staff/pupil training, and incident management. • Maintains online safety incident logs and liaises with external agencies (LA safeguarding partners, CEOP, Police, UK Safer Internet Centre). • Works with technical support to review filtering/monitoring effectiveness and reports to SLT and governors each term.
--	---

Governing Body	• Approves this policy and holds leaders to account for effective online safety. • Receives regular assurance on filtering/monitoring, including outcomes of the DfE self-assessment and annual effectiveness review.
Technical Support (Gateshead ICT Services / managed provider)	• Implements secure network configuration, patching, anti-malware, back-ups and access controls. • Operates and maintains filtering and monitoring solutions; prevents bypass (e.g. VPN/proxy); enables SafeSearch/YouTube Restricted Mode where feasible. • Keeps technical documentation and change logs; supports audits and tests of effectiveness.
Teachers and Support Staff	• Embed online safety across the curriculum, mapped to Education for a Connected World. • Teach pupils how to report concerns and critically evaluate online information (including mis/disinformation and AI-generated content).

All Staff and Volunteers	• Model safe, responsible and professional behaviour online; follow the Staff Acceptable Use Policy (AUP). • Supervise and guide pupils when using technology; report concerns to the DSL immediately and record on the school system. • Only use school-approved services and devices for pupil data and communications
Pupils	• Follow the Pupil AUP; keep personal information private; report anything that worries or upsets them. • Treat others with respect online and offline; do not circumvent filtering/monitoring.
Family Support Worker	• Educating Parents and raising awareness as instructed by Computing Coordinator
Parents/Carers	• Reinforce safe use at home; engage with school guidance and agree the Home school agreement which can be found on the website. • Use reporting routes (school/ CEOP/Police/ IWF) where concerns arise.
Visitors/External Agencies	Read and sign an AUP before using school systems; use consent images/data only with prior consent and in line with this policy.

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

6. Education, Curriculum & Staff Development

- Online safety is taught discretely and embedded across the curriculum (Computing/RSHE/PHSE), aligned to Education for a Connected World progression statements.
- Teaching covers: privacy and security; respectful relationships; managing online information; media literacy; copyright; reporting routes; financial scams; and AI literacy (benefits, limitations, risks and safe use).
- We use appropriate resources (e.g., Project EVOLVE) and respond to emerging local and national trends.
- Annual staff training includes filtering/monitoring responsibilities, data protection, AI guidance, and handling self-generated sexual imagery incidents.

7. Filtering & Monitoring

- School leaders and the DSL understand how filtering and monitoring operate and receive regular reports and alerts.
- Provision is reviewed at least annually and after significant incidents/changes. Findings are reported to governors with actions.
- Filtering aims to block illegal, harmful and inappropriate content without unreasonably impacting teaching and learning; monitoring provides proportionate oversight of user activity to identify risk and trigger safeguarding responses.
- Systems include measures against circumvention (e.g., VPN/proxy) and enable Safe Search/Restricted Mode where feasible, across school and BYOD where applicable.
- Illegal content (e.g., CSAM/terrorist material) is always blocked; any encounter is reported immediately to Police/CEOP/IWF as appropriate.
- We complete DfE "Plan technology for your school" self-assessments and act on recommendations.

8. Data Protection & Information Security

- Access to systems is role-based and protected by strong, unique passwords and (where available) MFA.
- Pupil/staff personal data is processed lawfully and stored only on school-approved services/devices; portable media is encrypted.
- Only approved cloud platforms are used for pupil data. Staff never use personal accounts for school business.

9. Use of Email, Communication & Collaboration Tools

- Staff use school-issued accounts for all professional communication. Tone is professional; messages may be audited/retained.
- Staff do not communicate with pupils via personal email/messaging/social media.
- Chain emails, phishing and suspicious links are reported and not forwarded.

10. Website, Social Media & Publishing

- The website complies with DfE requirements. Pupil images are used only with consent; no full names alongside images.
- Class blogs/learning platforms use school systems with appropriate access controls.
- Staff maintain clear separation between personal and professional online presence; they must not discuss pupils, parents or colleagues on personal accounts.

11. Use of Images, Video & Audio

- Only school devices are used to capture or store images/audio of pupils.
- Images must be appropriate; avoid settings that could cause embarrassment or risk.
- Parental consent is checked before sharing; storage and retention follow data protection policies.

12. Mobile Devices & Personal Equipment

- Staff personal devices are used only in non-pupil areas and never to store pupil data or images.
- Pupils may bring phones only by agreement; devices are switched off and stored securely during the school day.

13. Managing Online Safety Incidents

- Concerns are reported immediately to the DSL and recorded on the school system. Urgent risks are escalated to Police/Children's Services as necessary.
- Illegal or harmful content encountered online is reported to Police/CEOP/IWF as appropriate. Staff never investigate or copy illegal content.
- For self-generated sexual imagery involving pupils, the DSL follows national guidance, records actions and informs parents where appropriate.
- Pupils and parents are signposted to Report Remove (Childline/IWF) to support the removal of nude/semi-nude images online.

14. Working with Parents/Carers & Community

We provide regular updates, workshops and guidance to help families manage online safety at home, including device controls, gaming, social media and reporting routes. Parents/carers are asked to sign the Home-School Agreement and Pupil AUP each year.

15. Safeguarding, Behaviour & Disciplinary Measures

Online safety concerns are addressed through the school's safeguarding, behaviour and anti-bullying procedures. Searching, screening and confiscation are managed in line with DfE guidance and school policy. Sanctions are proportionate and focus on education and restoration alongside safeguarding.

Appendix A – Staff & Volunteer Acceptable Use Policy (AUP)

- I will use school systems, devices and accounts responsibly and only for professional purposes.
- I will keep passwords private and use only my own credentials; I will enable MFA where provided.
- I will only store/process data on approved services/devices and will encrypt portable media.
- I will not use personal devices/accounts to contact pupils or parents; I will use school-approved platforms only.
- I will use only school devices to capture images/audio of pupils and only with appropriate consent.
- I will report safeguarding concerns, technical security incidents or policy breaches immediately to the DSL/IT support.
- I will complete annual safeguarding and online safety training, including filtering/monitoring responsibilities and safe/ethical AI use.

Signature: _____ Date: _____ Name (print): _____

Appendix B – Pupil & Parent/Carer Acceptable Use Agreement

- I will keep my personal information private and my passwords secret.
- I will be kind and respectful online and will not bully or hurt others with my words or images.
- I will not try to visit blocked websites or use tools to get around school filters.
- If something online worries or upsets me, I will tell an adult straight away.
- I understand that school systems are monitored to help keep everyone safe.

Parent/Carer: I will support my child's safe use of technology at home and work with the school to resolve concerns. I consent to appropriate use of images in line with school policy (where opted).

Pupil signature: _____ Parent/Carer signature: _____ Date: _____

Appendix C – Filtering & Monitoring Statement

- Provider/arrangements: LA-approved filtered broadband with safeguarding-grade web filtering; device monitoring on managed endpoints; classroom supervision and screen-viewing as part of our monitoring strategy.
- Governance: Leaders/DSL receive regular reports; governors are updated termly. An annual review and real-world effectiveness test is completed and recorded.
- Configuration: Illegal material is always blocked; Safe Search/Restricted Mode enforced where feasible; circumvention is actively prevented; categories reviewed regularly with curriculum needs in mind (avoid over-blocking).
- Self-assessment: The DfE "Plan technology for your school" self-assessment is completed and recommendations are actioned.

Appendix D – Online Safety Incident Workflow (Summary)

1. ****Identify & secure****: Stop the activity; do not forward/copy suspicious or illegal material; preserve evidence/screens where lawful and safe.
2. ****Report to DSL immediately****: Record on the school safeguarding system (include time, device, users, URLs/apps).
3. ****Immediate risk?****: Contact Police/Children's Services. For online sexual abuse/grooming, submit a report to CEOP. For suspected child sexual abuse imagery, report to the IWF.
4. ****Contain & support****: Apply technical blocks; engage parents/carers as appropriate; provide pastoral support to pupils involved.
5. ****Decide & act****: DSL follows national guidance (including for self-generated sexual imagery), sets actions and sanctions proportionate to age/need.
6. ****Review & learn****: Update risk assessment, complete DfE self-assessment actions if technical lessons emerge; report to governors.

Appendix E – References (key national guidance)

- Keeping Children Safe in Education (KCSIE) 2025 – DfE (statutory guidance).
- DfE: Meeting digital and technology standards – Filtering and Monitoring (core standard).
- DfE: Plan technology for your school (self-assessment service).
- Education for a Connected World – UKCIS framework.
- DfE: Generative AI in education – policy paper and support materials for leaders.
- NSPCC Learning: KCSIE 2025 summary of changes (online safety risk additions).
- UK Safer Internet Centre: Updates to Filtering & Monitoring Standards (2024) and KCSIE 2025 filtering/monitoring expectations.
- Childline/Internet Watch Foundation: Report Remove (for young people).
- CEOP Safety Centre (report online sexual abuse).

Incident Workflow

