

Settrington All Saints' C E Primary School
Online Safety Policy



This policy was last reviewed	November 2025
Next review date	November 2026

This policy should be read alongside Settrington All Saints Primary School policies and procedures on child protection and safeguarding.

Online Safety & AI Policy

Applies to: All staff, volunteers, pupils, parents/carers, governors, contractors, and visitors using school ICT systems or devices.

Purpose

Settrington All Saints' C E Primary School is committed to safeguarding pupils in an increasingly digital world. This policy sets out how we manage online safety, including Artificial Intelligence (AI), in line with KCSIE 2025 and related DfE expectations for filtering, monitoring, and cyber resilience. It aims to prevent harm, ensure compliance with UK GDPR, and promote responsible, educationally beneficial use of technology.

This policy covers:

- School networks, internet services, devices (including loaned devices), wireless access, filtering and monitoring systems.
- Use of online services, platforms, apps, and AI tools in teaching, learning, and school operations.
- Off-site use where school systems/data are accessed (e.g., remote learning, trips, extracurricular activities).

Legal & Guidance Framework

- **KCSIE 2025** (statutory): online safety, filtering & monitoring, and expanded online harm categories.
- **NSPCC CASPAR briefing on KCSIE 2025**: implementation highlights (misinformation/disinformation, AI guidance signposts, and governance).
- **UK GDPR** and school data protection policies (lawful processing, security, data minimisation).

Definitions & Risk Categories (4Cs)

We adopt the KCSIE "4Cs" model:

- **Content**: exposure to illegal/inappropriate/harmful material (e.g., pornography, extremism, misinformation, disinformation and conspiracy theories)
- **Contact**: harmful online interaction/grooming

- **Conduct:** harmful behaviour (e.g., cyberbullying, sharing nudes/semi-nudes)
 - **Commerce:** scams, gambling, phishing, financial exploitation
- Policy wording and curriculum reflect these risks and teach pupils critical evaluation of online content and AI outputs.

Roles & Responsibilities

- **Headteacher/DSL (Designated Safeguarding Lead): Caryl Shephard**
Leads online safety strategy and implementation; oversees AI risk assessments; ensures compliance with KCSIE; ensures reporting/escalation; coordinates staff training; provides termly safeguarding reports to governors.
- **Deputy DSL(s): Kate Hind**
Support incident response, recording, and liaison with agencies.
- **Online Safety Coordinator: DSL**
Coordinates education programme, parent engagement, and routine monitoring checks.
- **Service Provider: NYES Digital**
Implements filtering/monitoring, cyber controls, incident response measures; maintains evidence of reviews/settings; ensures systems align with DfE expectations.
- **Safeguarding Governor: Cate Turner**
Provides strategic oversight; receives termly reports; challenges and supports compliance; signs off annual filtering/monitoring review evidence.
- **All Staff & Volunteers:**
Model safe practice; follow Acceptable Use Policy (AUP); supervise pupil access; report concerns immediately to DSL; complete training.
- **Parents/Carers:**
Support the school's online safety approach; follow parent AUP; attend workshops; raise concerns.
- **Pupils:**
Follow pupil Acceptable Use Policy; use technology responsibly; report anything worrying.

Preventive Controls: Filtering, Monitoring & Cybersecurity

Filtering & Monitoring

- School devices and networks are protected by appropriate web filtering and user activity monitoring proportionate to age, curriculum, and risk.
- **Annual review:** DSL and Safeguarding Governor review effectiveness at least once per year; document settings, exceptions, rationales, incident logs, and actions. Evidence retained in the **Online Safety Evidence:** (policy, minutes, risk assessments, audit trail).
- **Leadership understanding:** HT and governors maintain oversight of how systems work, what they flag, and how alerts are responded to.

Cybersecurity

- Maintain proportionate technical and organisational measures (patching, MFA where feasible, strong passwords, role-based access, encrypted storage, secure backups).
- **Incident response:** clear steps for containment, investigation, safeguarding impact assessment, communication, and restoration.
- Incorporate cybersecurity into staff training (including phishing awareness and reporting).

Artificial Intelligence (AI) — Safe Use

Principles

- **Educational benefit only**; AI never replaces professional judgement.
- **Risk assessment** before adoption to ensure AI cannot bypass filtering/monitoring and does not require unnecessary personal data.
- **Supervised access**: pupils use school-approved AI tools only under staff supervision.
- **Data protection**: do not upload personal/sensitive pupil data to external AI; comply with UK GDPR.
- **Content safety**: staff must check AI outputs for accuracy, age-appropriateness, bias, and potential harm before use with pupils.
- **Assessment integrity**: pupils must **not** use AI to complete assessed work unless explicitly authorised; staff should design tasks to discourage misuse.

Governance

- AI tools, purpose, age group, risk assessment, controls will be assessed by DSL and use, incidents, and mitigations reported termly to governors within the safeguarding report.

Education: Curriculum & Digital Literacy

- Embed digital literacy within Computing and PSHCE schemes of work (critical thinking, fact-checking, recognising bias/misinformation, respectful conduct, privacy/security).
- Teach the 4Cs risks and safe use of search engines, generative AI, and collaboration tools; include age-appropriate lessons and reporting pathways consistent with KCSIE.
- Termly review of objectives; targeted interventions where risk indicators arise.

Parent/Carer Engagement

- Regular NSPCC/online safety workshops; bulletins on curriculum tools (e.g., Scratch, Times Tables Rock Stars), filtering/monitoring at school, and tips for the home.
- Provide Acceptable Use Policy and guidance on misinformation/disinformation and safe AI use at home; signpost reputable resources.

Procedures: Reporting, Recording & Escalation

Immediate Response

If staff become aware of harmful content, contact/grooming, bullying, AI misuse, or a cyber incident:

1. Ensure pupil safety (remove from risk; preserve evidence where possible).
2. Report to DSL immediately (verbally) and submit a written record.
3. Record in the school safeguarding system (e.g., CPOMS) with actions taken.
4. DSL assesses and escalates to children's social care/police where required; liaises with parents/carers as appropriate.

Online Abuse & Harmful Sexual Behaviour

Follow KCSIE guidance and school child protection procedures; provide support for victim(s); address behaviour; review filtering/monitoring if applicable.

Cyber Incidents

- Teaching staff initiate containment and technical investigation; DSL assesses safeguarding impact; report notifiable breaches in line with data protection procedures; document lessons learned. Inform NYES Digital and IT support.

Training & Awareness

- Induction: all staff receive online safety and AI/cyber awareness on joining.
- Annual training: covers KCSIE updates, 4Cs risks, filtering/monitoring, cyber hygiene, AI boundaries, reporting pathways.
- Refreshers/briefings: issued following incidents, new guidance, or technology changes.

Monitoring, Audit & Review

- Termly: DSL reports online safety and AI matters to governors via Safeguarding governor (incidents, trends, mitigations).
- Annually: documented review of filtering/monitoring effectiveness; update risk assessments; policy review each Autumn Term or sooner following KCSIE/DfE updates.
- Maintain Online Safety Evidence in Safeguarding documentation (policy, AUPs, minutes, risk assessments, training logs, incident logs, action plans).

Acceptable Use (AUP) - Summary

- **Staff/Volunteers:** Use school devices/accounts for professional purposes; protect credentials; do not upload personal/sensitive pupil data to external AI; report concerns immediately.
- **Pupils:** Use technology respectfully; follow instructions; never share personal details; only use AI tools when a teacher says so; report anything worrying.
- **Parents/Carers:** Support pupil safe use; follow school guidance; engage with workshops; raise questions with the school.

(Full AUPs are maintained and issued separately.)

Related Policies & Guidance

- Child Protection & Safeguarding Policy
- Behaviour Policy; Anti-Bullying Policy
- Data Protection & Records Management
- Staff Code of Conduct; Mobile/Device Policy
- Photography & Image-Sharing Guidance

Named Contacts

- **Online Safety Coordinator / DSL:** Caryl Shephard
Email: headteacher@settrington.n-yorks.sch.uk
- **Safeguarding Governor:** Rev Cate Turner
Email: cturner@settrington.n-yorks.sch.uk