

Bolton-on-Swale St Mary's CE Primary School

‘To Love, Live and Learn together’

Online Safety and Acceptable Use Policy

Policy Review Date:	September 2026
Next Review Date:	September 2027
Designated Safeguarding Lead (DSL):	Headteacher / DSL
Online Safety Governor:	Chair of Governors / Safeguarding Governor

1. Introduction and Christian Ethos

At Bolton-on-Swale St Mary's CE Primary School, our Christian values underpin our vision for nurturing a community where every individual is valued. In a fast-changing digital landscape, we aim to equip our pupils with the skills, wisdom, and resilience to use technology safely, creatively, and responsibly. This policy outlines our collaborative approach to protecting our children while empowering them to become positive digital citizens.

2. Policy Scope and Links

This policy applies to all members of the school community—including staff, pupils, governors, volunteers, and parents—who have access to or use school digital technology, or whose personal technology use impacts the school ecosystem. It aligns closely with the Department for Education's (DfE) statutory guidance, including 'Keeping Children Safe in Education' (KCSIE), and links explicitly with our Safeguarding & Child Protection Policy, Anti-Bullying Policy, Behaviour Policy, and Staff Code of Conduct.

3. Roles and Responsibilities

3.1 Governing Body

- **Strategic Oversight:** Ensuring a safe online environment through robust strategic oversight.
- **Filtering & Monitoring:** Ensuring that web filtering and monitoring mechanisms are highly effective and checked regularly in accordance with national filtering guidelines.

3.2 The Headteacher and Designated Safeguarding Lead (DSL)

- **Ultimate Accountability:** Holding ultimate operational accountability for online safety across the school.

- **Incident Management:** Processing all online safety and cyberbullying logs, identifying trends, and applying interventions.
- **Staff CPD:** Ensuring staff undergo regular, up-to-date safeguarding training that covers digital threats, artificial intelligence, and online grooming.

3.3 Teaching and Support Staff

- **Supervision:** Actively supervising pupils whenever they are utilizing digital devices or internet services on school property.
- **Curriculum Integration:** Delivering a structured online safety curriculum that embeds digital literacy across all subjects.
- **Reporting:** Instantly reporting any online safety flags, suspicious behaviour, or disclosures to the DSL via the school's safeguarding software.

4. Infrastructure: Filtering, Monitoring, and AI Usage

4.1 Technical Defences

The school employs a robust, age-appropriate internet filtering and monitoring framework to block illegal, inappropriate, or harmful content. This is Smoothwall. Staff and pupils access the network via unique, secure user profiles. System logs are audited routinely to identify any search queries or activities that trigger safeguarding alerts.

4.2 Generative Artificial Intelligence (AI)

We recognize the educational potential of Generative AI tools, but we prioritize data protection and academic integrity. Pupils are not permitted to use AI tools unless under the direct instruction and strict supervision of a staff member. Staff utilizing AI tools for planning or resource generation must never input sensitive, personal, or identifiable pupil data into external AI platforms.

5. The Four Areas of Risk (DfE Guidance)

Our safety framework evaluates and tackles digital concerns through the lens of the DfE's defined risk vectors:

- **Content:** Exposure to illegal, violent, radicalizing, or age-inappropriate media and misinformation.
- **Contact:** Harmful interactions with unknown adults or malicious peers, including online grooming or exploitation.
- **Conduct:** Personal actions that cause harm, including cyberbullying, sharing inappropriate personal images, or digital footprint damage.
- **Commerce:** Exposure to financial risks, scams, phishing, aggressive in-game advertising, or online gambling.

6. Acceptable Use Policy (AUP) for Pupils

To ensure everyone stays safe and happy online, all pupils must remember the following rules:

- **Ask Permission:** I will always ask a teacher or adult before logging on to the internet at school.
- **Stay on Approved Sites:** I will only visit websites and apps that my teacher has approved for my lessons.
- **Keep Secrets Secret:** I will keep my passwords a secret and never try to log in as anyone else.
- **Be Kind Online:** I will always write polite, friendly, and encouraging messages to my classmates and teachers.
- **Tell an Adult:** I will tell an adult immediately if I see anything online that makes me feel uncomfortable, scared, or sad.
- **Personal Devices:** I will leave my personal smartphone or smartwatch at home and not bring these to school. I will ask an adult at home to help me to use them safely and responsibly.

7. Incident Management and Reporting

When an online safety violation or safeguarding breach is identified, the school will act swiftly using a standardized response plan:

- 1. Secure and Isolate:** The immediate threat or distress is neutralized. The affected device is turned off or isolated, and the child's well-being is prioritised.
- 2. Log and Inform:** The details of the incident are recorded objectively and submitted to the DSL. Parents are contacted to explain what occurred and how it is being addressed.
- 3. Investigate and Apply Sanctions:** The school investigates the root cause. Behavioural sanctions are applied consistently in accordance with the school Behaviour Policy.
- 4. Escalate Externally:** If the incident involves illegal content, online exploitation, or severe threat, the school immediately escalates the matter to the local authorities, police, or CEOP.

Community Partnership: Online safety relies heavily on a unified approach between home and school. We regularly share educational resources, newsletters, and safety guides with parents to help protect children across both environments.