Online Safety Policy

Written: March 2026
Review: March 2027
Written by: George Lumley

Update - September 2026:

- Section 6 - Smoothwall now being used in school
- Section 14 - Artificial Intelligence

At St Margaret's CE Primary School, our Christian vision *Created to Shine* and our values of *Love* and *Aspire* shape every aspect of school life, including how we keep children safe online. We believe every child is uniquely created, precious, and capable of flourishing. Online safety is therefore an essential part of our safeguarding culture: we teach children to act with love, wisdom, and respect online; we aspire to equip them with the skills to navigate the digital world confidently; and we work in partnership with families to ensure all pupils can shine safely in an increasingly connected world.

Purpose:

This policy sets out how the school fulfils its statutory duties under Keeping Children Safe in Education, the DfE statutory guidance, and relevant legislation to protect pupils from online harm. It explains expectations for staff, pupils, parents, governors, and visitors, and outlines how online safety is taught, monitored, and embedded across the curriculum and wider school life.

3. Statutory and Regulatory Framework

This policy is informed by the following statutory and regulatory documents:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- Education Act 2002
- The Prevent Duty
- UK GDPR and Data Protection Act 2018
- Ofsted Education Inspection Framework
- DfE *Teaching Online Safety in Schools*
- DfE *Filtering and Monitoring Standards*

This policy should be read alongside the school's Safeguarding & Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, and Acceptable Use Agreements.

4. Roles and Responsibilities

4.1 Governing Body

The Governing Body ensures the school complies with statutory online safety duties, including appropriate filtering and monitoring systems, staff training, and curriculum provision. Governors receive regular reports on online safety incidents, trends, and actions.

4.2 Headteacher

The Headteacher holds overall responsibility for online safety, ensuring policies are implemented, staff are trained, and systems are effective. The Headteacher ensures online safety is part of the school's safeguarding culture and strategic planning.

4.3 Designated Safeguarding Lead (DSL)

The DSL leads on online safety within safeguarding with the Headteacher, including:

- responding to online safety concerns
- liaising with external agencies

- ensuring staff understand online risks
- maintaining accurate records
- ensuring filtering and monitoring meet DfE standards - supported by our School Business Manager.

4.4 All Staff

All staff must:

- follow the Staff Code of Conduct and Acceptable Use Agreement
- complete regular online safety training
- report concerns immediately to the DSL through CPOMS
- model safe, respectful online behaviour
- use school devices and systems responsibly

4.5 Pupils

Pupils are taught to:

- use technology safely, respectfully, and responsibly
- report concerns to a trusted adult
- understand the impact of online behaviour
- protect personal information
- engage positively with the digital world

4.6 Parents and Carers

Parents are encouraged to:

- support the school's online safety approach
- monitor their child's online activity at home
- engage with school workshops and guidance
- report concerns to the school

5. Education and Curriculum

Online safety is embedded across the curriculum, including Computing, PSHE, RSE, and collective worship. Teaching is age-appropriate, inclusive, and aligned with DfE guidance.

Pupils learn about:

- healthy online relationships
- cyberbullying and respectful communication
- privacy, security, and digital footprints
- misinformation and critical thinking
- online gaming and social media risks
- reporting routes and help-seeking

The school uses a progressive curriculum that builds knowledge year-on-year and reflects emerging risks. - See PSHE and Computing curriculum documentation.

6. Filtering and Monitoring

The school uses filtering and monitoring systems which:

- block harmful or inappropriate content
- monitor online activity for safeguarding concerns
- provide alerts to the DSL where necessary
- are reviewed regularly for effectiveness

As of September 2026, the school use Smoothwall as our internet filtering and monitoring system alongside SurfProtect.

Staff are trained to understand the limitations of filtering and monitoring and the importance of supervision and vigilance. Reminders are sent out in staff bulletins to ensure training is kept fresh.

Alerts of a safeguarding concern are recorded on CPOMS and actioned in accordance with our safeguarding procedures.

An activity of concern is investigated and actioned in accordance with our policies and procedures for safeguarding and behaviour.

7. Use of School Devices and Networks

All staff and pupils must use school devices, email accounts, and networks in line with the school's Acceptable Use Agreements. Personal devices must not be used to store or transmit school data. Staff must only use school-approved platforms for communication with pupils and families.

8. Remote Learning

Where remote learning is used, the school ensures:

- safeguarding principles remain central
- communication is professional and secure
- platforms are approved and monitored - at St Margaret's School we use Seesaw for this.
- parents are supported to keep children safe at home

9. Managing Online Safety Incidents

All online safety concerns must be reported immediately to the DSL. The school will:

- follow safeguarding procedures
- involve external agencies where necessary
- record incidents accurately
- support pupils and families
- take disciplinary action where appropriate
- review practice to prevent recurrence

Incidents may include cyberbullying, online grooming, exposure to harmful content, sexting, radicalisation concerns, or breaches of data security. CPOMS is used by staff to record and report these concerns.

10. Cyberbullying

Cyberbullying is treated with the same seriousness as face-to-face bullying. The school will:

- investigate all reports
- support victims
- work with families
- apply sanctions where appropriate
- educate pupils about respectful behaviour

Cyberbullying is also covered in our curriculum teaching to ensure children know about the dangers of this and how to keep themselves safe online.

11. Data Protection and Privacy

The school complies with UK GDPR and the Data Protection Act 2018. Personal data is processed securely, and staff and governors receive training on data protection, secure passwords, and safe information handling.

12. Staff Training

All staff and governors receive annual safeguarding training that includes online safety. Additional training is provided for the DSL, senior leaders, and staff with specific responsibilities. Training covers:

- emerging online risks
- digital safeguarding
- Prevent and radicalisation
- reporting procedures
- safe professional conduct

13. Partnership with Parents

The school works closely with parents through workshops, newsletters, website guidance, and signposting to reputable resources. Parents are encouraged to maintain open conversations with their children about online behaviour and safety.

14. Artificial intelligence (AI)

The use of AI forms part of the school's wider safeguarding and online safety arrangements. All staff must remain alert to safeguarding risks arising from generative AI, AI chatbots, synthetic media, deepfakes, AI-generated intimate imagery, misinformation and online manipulation. A separate Use of AI in School policy has been written and must be followed.

15. Monitoring and Review

This policy is reviewed annually by the Headteacher and Governing Body, or sooner if required by changes in legislation, technology, or safeguarding needs.