St Margaret’s CE VA Primary School: Online Safety Policy

Policy Status: Statutory

Date Implemented: June 2025

Date Reviewed: June 2025

Next Review Date: June 2026

1. Introduction

This Online Safety Policy outlines St Margaret’s CE VA Primary School's commitment to providing a safe and secure online environment for all pupils, staff, parents, and visitors. It aims to protect our community from online risks and promote responsible technology use, aligning with our Christian values of respect, responsibility, and truthfulness. This policy is underpinned by the principles outlined in Keeping Children Safe in Education (KCSiE) 2024 and other relevant legislation.

2. Purpose

The purpose of this policy is to:

- Safeguard pupils and staff from potential harm and inappropriate online material.
- Educate pupils about responsible and safe online behaviour.
- Establish clear procedures for identifying, reporting, and addressing online safety concerns.
- Ensure compliance with relevant legislation and guidance.
- Promote a culture of online safety awareness across the whole school community.

3. Legal Framework and Guidance

This policy is informed by and compliant with the following legislation and guidance:

- Keeping Children Safe in Education (KCSiE) 2024
- The Prevent Duty
- General Data Protection Regulation (GDPR)
- The Children Act 1989 and 2004
- Education Act 2002
- Counter-Terrorism and Security Act 2015
- Online Safety Act (when enacted)

4. Roles and Responsibilities

- **Governing Body:**
    - Ensuring the school has an effective online safety policy.
    - Regularly reviewing the policy's implementation and effectiveness.
    - Allocating sufficient resources for online safety measures.
- **Headteacher:**
    - Overall responsibility for the implementation of the online safety policy.
    - Ensuring staff are trained and aware of their responsibilities.
    - Reporting online safety incidents to the governing body.
- **Designated Safeguarding Lead (DSL):**
    - Leading on all safeguarding matters, including online safety.
    - Providing advice and support to staff on online safety concerns.
    - Liaising with external agencies as necessary.
- **IT Manager/Technician:**
    - Implementing and maintaining appropriate filtering and monitoring systems.
    - Ensuring the school's IT infrastructure is secure.
    - Providing technical support for online safety issues.
- **Teachers and School Staff:**
    - Promoting responsible online behaviour among pupils.
    - Monitoring pupils' online activity and reporting any concerns.
    - Integrating online safety education into the curriculum.
- **Pupils:**
    - Using technology responsibly and safely.
    - Reporting any online safety concerns to a trusted adult.
    - Following the school's online safety rules.
- **Parents/Carers:**
    - Supporting the school's online safety policy at home.
    - Supervising their child's online activity.
    - Reporting any online safety concerns to the school.

5. Online Safety Education

- **Curriculum Integration:** Online safety will be embedded across the curriculum, particularly in computing, PSHE, and citizenship lessons.
- **Age-Appropriate Content:** Online safety education will be tailored to the age and developmental stage of pupils.

- **Key Topics:** The curriculum will cover the following topics:
    - Responsible online behaviour and digital citizenship.
    - Cyberbullying and online harassment.
    - Privacy and data security.
    - Critical evaluation of online information (fake news).
    - Safe use of social media and online gaming.
    - Recognising and reporting online abuse and exploitation.
    - Understanding the risks of sharing personal information online.
    - The 4 C's: Content, Contact, Conduct, Commerce
- **Resources:** The school will use a range of resources, including:
    - UK Safer Internet Centre materials.
    - Childnet International resources.
    - NSPCC resources.
    - Assemblies and workshops.
- **SWITCH Team:** The SWITCH (See World Issues through Christian Hearts) Team will be involved in promoting online safety awareness and developing resources.

6. Acceptable Use of Technology

- **Pupil Acceptable Use Agreement:** All pupils will be required to sign an acceptable use agreement outlining the school's expectations for responsible technology use.
- **Staff Acceptable Use Agreement:** All staff will be required to sign an acceptable use agreement outlining the school's expectations for responsible technology use.
- **Mobile Phone and Smart Technology Policy:**
    - Clear guidelines on the use of mobile phones and smart technology on school premises.
    - Restrictions on the use of mobile phones during lessons.
    - Procedures for confiscating mobile phones if misused.
    - Address issues such as cyberbullying, sharing indecent images, and viewing harmful content.
- **Use of School Devices and Networks:**
    - Clear guidelines on the use of school computers, laptops, tablets, and internet access.
    - Restrictions on accessing inappropriate websites and content.
    - Procedures for reporting technical issues.

7. Filtering and Monitoring

- **Filtering Systems:** The school will implement appropriate filtering systems to block access to harmful and inappropriate content.

- **Monitoring Systems:** The school will implement monitoring systems to track pupils' online activity and identify potential risks.
- **Regular Review:** The effectiveness of filtering and monitoring systems will be reviewed at least annually.
- **Escalation Procedures:** Clear procedures for escalating concerns identified through monitoring.
- **Proportionality:** The proportionality of costs versus safeguarding risks will be considered when selecting filtering and monitoring systems.
- **Transparency:** Parents and carers will be informed about the school's filtering and monitoring systems.
- **Compliance:** Ensure filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).
- **Department for Education's filtering and monitoring standards:**
    - identify and assign roles and responsibilities to manage filtering and monitoring systems.
    - review filtering and monitoring provision at least annually.
    - block harmful and inappropriate content without unreasonably impacting teaching and learning.
    - have effective monitoring strategies in place that meet their safeguarding needs.

8. Responding to Online Safety Incidents

- **Reporting Procedures:** Clear procedures for reporting online safety incidents, including cyberbullying, online abuse, and exposure to inappropriate content.
- **Investigation Procedures:** Procedures for investigating online safety incidents and taking appropriate action.
- **Support for Victims:** Support for pupils who have been victims of online safety incidents.
- **Sanctions for Offenders:** Sanctions for pupils who have engaged in harmful online behaviour.
- **External Agencies:** Procedures for liaising with external agencies, such as the police and social services.
- **Record Keeping:** Accurate records of all online safety incidents will be maintained.

9. Remote Education

- **Safeguarding During Remote Learning:** This policy applies equally to remote education settings.
- **Communication with Parents:** Regular communication with parents about online safety during remote learning.
- **Monitoring and Support:** Strategies for monitoring pupils' online activity and providing support during remote learning.

- **Training:** Staff will receive training on safeguarding pupils during remote learning.
- **Guidance:** Safeguarding and remote education – GOV.UK (www.gov.uk) and Providing remote education: guidance for schools – GOV.UK (www.gov.uk).

10. Partnership with Parents/Carers

- **Parent Information Sessions:** Regular information sessions for parents on online safety.
- **Online Safety Resources:** Providing parents with access to online safety resources and guidance.
- **Communication Channels:** Establishing clear communication channels for parents to report online safety concerns.
- **Parental Involvement:** Encouraging parents to be actively involved in their child's online safety education.
- **Awareness:** Parents and carers are likely to find it helpful to understand what systems schools and colleges use to philtre and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

11. Policy Review and Evaluation

- **Annual Review:** This policy will be reviewed annually by the governing body and the DSL.
- **Stakeholder Feedback:** Feedback will be sought from pupils, staff, and parents during the review process.
- **Policy Updates:** The policy will be updated to reflect changes in legislation, guidance, and best practises.
- **Monitoring Effectiveness:** The effectiveness of the policy will be monitored through incident reports, pupil surveys, and staff feedback.

12. Training

- **Staff Training:** All staff will receive regular training on online safety, including safeguarding, data protection, and responsible technology use.
- **DSL Training:** The DSL will receive specialist training on online safety issues.
- **Pupil Training:** Pupils will receive age-appropriate training on online safety as part of the curriculum.
- **Governor Training:** Governors will receive training on their responsibilities related to online safety.

13. Useful Contacts and Resources

- **Childline:** 0800 1111
- **NSPCC:** 0808 800 5000

- **UK Safer Internet Centre:** https://saferinternet.org.uk/
- **Childnet International:** https://www.childnet.com/
- **Internet Watch Foundation:** https://www.iwf.org.uk/
- **Report to the Anti-Phishing Working Group (https://apwg.org/)**

This policy is a working document and will be reviewed and updated regularly to ensure it remains relevant and effective.