



# St Mary's C of E (VA) Primary School

Working together  
in an inclusive Christian environment  
to allow every pupil to shine brighter and brighter.

St Mary's is an inclusive school where we believe that all people are of equal value, irrespective of their ethnicity, culture, religion, gender, ability or sexual identity. We recognise and respect differences.

## Online Safety

This policy is GDPR compliant.

Date of issue: February 2026

Last reviewed/adopted: June 2026 (Standards and Ethos)

Next review date: Summer 2028

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

# St Mary's C.E. Primary School

## ONLINE SAFETY POLICY

### Including Acceptable Use Agreements

#### 1. Introduction

St Mary's C.E. Primary School recognises that internet, mobile, AI and digital technologies provide valuable opportunities for teaching, learning, socialisation and communication. At the same time, these technologies bring potential risks. This policy sets out how the school ensures that pupils, staff, governors, parents/carers and visitors use digital technologies safely and responsibly.

Online safety is part of the school's wider safeguarding responsibilities and applies to everyone in the school community. The policy should be read alongside safeguarding, behaviour, data protection, anti-bullying, and curriculum policies.

#### 2. Responsibilities

The governing board and headteacher have overall responsibility for ensuring online safety is monitored and embedded throughout the school.

The Designated Safeguarding Lead (DSL) is the named online safety lead, supported by senior leaders. The DSL is responsible for responding to safeguarding concerns linked to online use.

Staff must act as role models in safe use of technology, follow this policy, and teach pupils how to use digital technologies safely.

Pupils must follow the Acceptable Use Agreements and report anything that worries them online.

Parents/carers are expected to support the school's approach to online safety and reinforce safe use at home.

Visitors, volunteers and contractors must follow the school's online safety and acceptable use procedures.

### 3. Scope of Policy

This policy applies to:

- All pupils, staff and governors
- Parents/carers
- Visitors, volunteers, contractors and partner organisations using school systems or devices

It applies to all use of digital technologies on the school site and any use off site that could affect the safety or reputation of the school or its community.

The policy also covers remote education and hybrid learning.

### 4. Policy and Procedure

Use of email:

- Staff and governors must only use school email accounts or approved platforms for school business.
- Pupils must use school-approved accounts for learning activities.
- Personal email accounts must not be used for school business.

Accessing sites and downloading:

- Staff must check websites, software or apps before recommending or using them with pupils.
- Pupils must only access approved sites.
- Copyright and licensing rules must be followed.

Storage and use of images:

- Consent must be obtained before publishing pupil images.
- Images must only be stored on approved school systems.
- Personal devices must not be used to take images of pupils.

Mobile phones and personal devices:

- Staff may only use personal devices in designated areas, never in the presence of pupils.
- Pupils must hand in phones/devices as per school rules.

- Parents may only use devices in designated areas and must not take photos of children other than their own, unless authorised.

#### New technologies and AI:

- Emerging technologies, including generative AI, will only be used if approved by the headteacher/DSL/DPO following a risk assessment.
- AI must never be used in ways that compromise safeguarding or data protection.

#### Filtering, monitoring and cybersecurity:

- The school uses filtering and monitoring systems in line with KCSIE and DfE requirements.
- Staff and pupils must not bypass filters.
- Phishing and scams must be reported immediately.

#### Reporting incidents:

- Inappropriate content, cyberbullying, harmful communications or safeguarding concerns must be reported immediately to a member of staff or the DSL.
- All incidents are logged.
- Staff and pupils must use strong passwords, enable multi-factor authentication where available, and never share login details.

### 5. Curriculum

Online safety is embedded in the curriculum across subjects, including Computing, PSHE, Relationships and Health Education. Pupils are taught:

- How to use technology safely, respectfully and responsibly.
- To understand risks such as cyberbullying, online grooming, fake news and extremism.
- To protect personal information and maintain privacy online.
- To build digital resilience and a positive online reputation.

### 6. Staff and Governor Training

All staff and governors receive regular training in online safety and safeguarding. Training needs are reviewed annually. New staff and governors must sign Acceptable Use Agreements at induction.

### 7. Working in Partnership with Parents/Carers

The school works with parents/carers to promote safe online use at home. Parents are provided with guidance, updates and workshops. Parents are asked to sign the pupil Acceptable Use Agreement annually with their child.

## 8. Records, Monitoring and Review

Online safety incidents are recorded and monitored. The DSL and governors review incident logs regularly. This policy is reviewed annually and updated as required to reflect changes in technology and guidance.

## 9. Appendices

Appendix A – Acceptable Use Agreement for Staff, Governors, Student Teachers, Peripatetic Teachers

Appendix B – Requirements for Visitors, Volunteers and Parent/Carer Helpers

Appendix C – Acceptable Use Agreement for Pupils

Appendix D – Parent/Carer Responsibilities (Summary)

Appendix E – Guidance on Responding to Cyberbullying

Appendix F – Guidance on Preventing and Responding to Negative Comments on Social Media