



# St Thomas More Catholic Primary School, Saffron Walden

## ONLINE SAFETY POLICY

Policy No. STM-062

|                            |                       |
|----------------------------|-----------------------|
| Unique Policy Reference No | <b>STM-009</b>        |
| Approved by (inc date)     | <i>Governing Body</i> |
| Date Version Approved      | <i>October 2026</i>   |
| Date next due for review   | <i>October 2027</i>   |
| Author (Document Owner)    | <i>Headteacher</i>    |

## **1. Introduction**

### **1.1 Commitment to Online Safety**

At St Thomas More Catholic Primary School, we are committed to creating a culture of safeguarding in which children are protected from harm both offline and online. We recognise that technology plays an essential role in education, communication, creativity and learning, and that it also presents risks that must be managed appropriately.

Online safety is an integral part of safeguarding and child protection. The school seeks to provide a safe and secure environment in which all members of the school community can benefit from technology whilst understanding how to manage risk and behave responsibly online.

To achieve this, the school implements:

- a) A whole-school approach to online safety
- b) Effective safeguarding procedures and reporting systems
- c) Appropriate filtering and monitoring systems
- d) Online safety education embedded throughout the curriculum
- e) Regular safeguarding and online safety training for staff, volunteers and governors
- f) Education for pupils regarding online relationships, digital citizenship and responsible technology use
- g) Support and intervention for pupils affected by online harm
- h) Procedures for responding to online safety incidents
- i) Ongoing engagement with parents and carers
- j) Measures to prevent access to illegal, harmful or inappropriate content

### **1.2 Scope**

This policy applies to all members of the school community, including:

- Pupils
- Teaching staff
- Support staff
- Volunteers
- Governors
- Contractors
- Visitors
- Parents and carers

The policy applies whenever digital technology is used for school purposes, whether on or off-site and whether accessed through school-owned or personal devices.

### **1.3 Behaviour Beyond School**

The Education and Inspections Act 2006 empowers Headteachers to regulate pupil behaviour beyond the school premises where such behaviour affects members of the school community or brings the school into disrepute. This includes incidents involving:

- Cyberbullying
- Online harassment
- Harmful social media activity
- Sharing inappropriate content

- Actions that place a child or others at risk

The Education Act 2011 provides additional powers relating to the searching and examination of electronic devices where appropriate.

#### 1.4 Responding to Concerns

Online safety incidents will be managed in accordance with:

- The Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy

Parents and carers will be informed of concerns where appropriate and in accordance with safeguarding procedures.

#### 1.5 Policy Review

This policy will be reviewed annually or sooner where required due to:

- Changes in legislation
- Changes in safeguarding guidance
- Technological developments
- Emerging online risks

## 2. LEGISLATION AND GUIDANCE

This policy should be read alongside the most current versions of:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- Relationships Education, Relationships and Sex Education (RSE) and Health Education Statutory Guidance
- Teaching Online Safety in Schools
- Education for a Connected World Framework
- Filtering and Monitoring Standards for Schools and Colleges
- Sharing Nudes and Semi-Nudes: Advice for Education Settings
- Harmful Online Challenges and Online Hoaxes Guidance
- UK GDPR
- Data Protection Act 2018
- Online Safety Act 2023
- The school's Child Protection and Safeguarding Policy
- Data Protection Policy
- Behaviour Policy
- Acceptable Use Policy

### **3. ONLINE SAFETY RISKS**

The school recognises that online risks generally fall into four categories:

#### **3.1 Content Risks**

Including exposure to:

- Inappropriate or harmful content
- Extremist material
- Violent content
- Hate content
- Misinformation and disinformation
- Content promoting harmful behaviours

#### **3.2 Contact Risks**

Including:

- Online grooming
- Child sexual exploitation
- Radicalisation
- Coercion and manipulation
- Unwanted contact from strangers
- Peer-to-peer abuse

#### **3.3 Conduct Risks**

Including:

- Cyberbullying
- Online harassment
- Abuse via gaming platforms
- Sharing of personal information
- Sharing of nudes and semi-nudes
- Harmful online challenges

#### **3.4 Commerce Risks**

Including:

- Scams
- Phishing
- Fraud
- Identity theft
- Unauthorised purchases
- Misleading advertising

## **4. ROLES AND RESPONSIBILITIES**

### **4.1 Governing Body**

The Governing Body is responsible for ensuring that:

- a) Online safety is effectively managed within the school.
- b) Appropriate filtering and monitoring systems are in place.
- c) Online safety forms part of safeguarding oversight.
- d) Staff receive appropriate training.
- e) Policies are reviewed regularly.

The Safeguarding Governor will:

- Meet regularly with the Designated Safeguarding Lead (DSL)
- Monitor anonymised safeguarding data
- Review online safety arrangements
- Receive assurance regarding filtering and monitoring
- Report to the Governing Body

### **4.2 Headteacher**

The Headteacher has overall responsibility for safeguarding and online safety and will ensure that:

- Appropriate policies and procedures are implemented.
- Staff understand their responsibilities.
- Resources are available to support effective online safety provision.

### **4.3 Designated Safeguarding Lead (DSL)**

The DSL will:

- a) Lead on online safety within safeguarding arrangements.
- b) Coordinate responses to online safety concerns.
- c) Maintain records of incidents and actions taken.
- d) Support and advise staff.
- e) Liaise with external agencies where required.
- f) Ensure safeguarding concerns arising online are managed appropriately.
- g) Provide reports to governors and senior leaders.
- h) Ensure online safety education is effective.

The DSL will maintain awareness of:

- Online grooming
- Exploitation
- Cyberbullying
- Sharing of nudes and semi-nudes
- Radicalisation
- Misinformation and disinformation
- Harmful online challenges
- Emerging technologies and risks

#### **4.4 Technical Support Provider**

The school's technical support provider will:

- a) Maintain the security of the school's technology infrastructure.
- b) Implement appropriate filtering and monitoring systems.
- c) Maintain access controls and permissions.
- d) Apply software updates and security patches.
- e) Support investigations relating to safeguarding concerns.
- f) Report technical concerns that may impact safeguarding.

#### **4.5 Staff and Volunteers**

All staff and volunteers must:

- a) Read and adhere to this policy and the Staff Acceptable Use Policy.
- b) Maintain professional standards online.
- c) Report concerns immediately to the DSL.
- d) Embed online safety within teaching and learning.
- e) Supervise pupils appropriately when using technology.
- f) Model safe and responsible online behaviour.
- g) Follow data protection procedures.
- h) Recognise signs of online abuse, exploitation and harm.
- i) Participate in required training.

#### **4.6 Pupils**

Pupils are expected to:

- a) Use technology safely and responsibly.
- b) Follow school rules relating to technology use.
- c) Respect others online.
- d) Protect personal information.
- e) Report concerns or inappropriate content to a trusted adult.
- f) Understand the difference between acceptable and unacceptable online behaviour.

#### **4.7 Parents and Carers**

Parents and carers have an important role in supporting online safety and are encouraged to:

- a) Discuss online safety with their children.
- b) Monitor and supervise online activity where appropriate.
- c) Use parental controls and privacy settings.
- d) Reinforce school online safety messages.
- e) Report concerns to the school promptly.
- f) Support age-appropriate technology use.

The school will support parents through newsletters, workshops, information events and online resources.

#### **4.8 Computing Lead**

The Computing Lead will work alongside the DSL Team to actively promote and support the effective application of this policy, including signposting the school, parents and children to current initiatives and guidance, as well as having oversight of the computing curriculum and associated online safety curriculums (e.g. in PSHE) so children are well prepared and supported in their understanding of online safety.

## **5. CURRICULUM**

Online safety education is embedded throughout the curriculum and taught through Computing, Relationships Education, Health Education and other relevant subjects.

Teaching will include:

- Respectful relationships
- Online relationships
- Digital citizenship
- Privacy and security
- Cyberbullying
- Online reputation
- Managing personal information
- Critical evaluation of online content
- Misinformation and disinformation
- Artificial intelligence
- Reporting concerns and seeking support

Online safety education will be age-appropriate and progressive across all year groups.

## **6. EDUCATION AND TRAINING**

### **6.1 Staff and Volunteers**

All staff and volunteers will receive:

- Online safety training during induction
- Regular safeguarding updates
- Ongoing professional development
- Guidance on emerging online risks

### **6.2 Governors**

Governors will receive appropriate safeguarding and online safety training to enable them to fulfil their oversight responsibilities.

### **6.3 Parents and Carers**

The school will provide information and guidance through:

- Newsletters
- Parent workshops
- Website resources
- National awareness campaigns

## **7. FILTERING AND MONITORING**

The school will maintain effective filtering and monitoring systems that:

- a) Protect pupils from harmful or inappropriate content.
- b) Help identify safeguarding concerns.
- c) Are age-appropriate and proportionate.
- d) Are reviewed regularly.
- e) Comply with relevant statutory guidance.

The school will:

- Maintain records of significant alerts and incidents.
- Investigate concerns promptly.
- Review filtering effectiveness regularly.
- Ensure key safeguarding staff understand the filtering and monitoring systems in use.

## **8. MOBILE TECHNOLOGIES**

The school recognises the importance of mobile technology while also understanding associated risks.

The school will:

- a) Establish clear expectations regarding mobile device use.
- b) Promote safe and responsible use.
- c) Teach pupils about risks associated with mobile technologies.
- d) Restrict photographing, recording or sharing content where inappropriate.
- e) Investigate misuse in line with safeguarding and behaviour procedures.

## **9. USE OF DIGITAL IMAGES AND VIDEO**

The school is committed to protecting the privacy, dignity and safety of pupils.

The school will:

- a) Obtain appropriate consent for the use of images.
- b) Ensure images are used appropriately and securely.
- c) Use school-approved devices for school photography and recording.
- d) Educate pupils about responsible sharing of images.
- e) Store images securely and in accordance with data protection requirements.

Parents and carers are strongly encouraged not to share images of other children on social media without the consent of the child's parent or carer.

## **10. ARTIFICIAL INTELLIGENCE (AI)**

The school recognises that artificial intelligence technologies are becoming increasingly accessible.

The school will:

- a) Teach pupils about the opportunities and risks associated with AI.
- b) Promote critical thinking when evaluating AI-generated content.
- c) Encourage ethical and responsible use of AI technologies.
- d) Ensure AI tools are used in a manner that supports learning and safeguarding.

Staff must not enter confidential, personal or sensitive information into public AI systems unless explicitly authorised and compliant with the school's data protection procedures. See associated policies around Acceptable Use, Computing and Data Handling.

## **11. DATA PROTECTION**

The school processes personal information in accordance with:

- UK GDPR
- Data Protection Act 2018
- School Data Protection Policy

All members of the school community are expected to handle personal information responsibly and securely.

## **12. SOCIAL MEDIA**

### **12.1 School Accounts**

Official school social media accounts will:

- a) Be authorised by the Headteacher.
- b) Be managed by designated members of staff.
- c) Be overseen by at least two authorised staff members.
- d) Operate in accordance with safeguarding and data protection requirements.
- e) Include clear reporting and moderation procedures.

### **12.2 Staff Use of Social Media**

Staff must:

- a) Maintain professional boundaries at all times.
- b) Follow the Staff Code of Conduct.
- c) Review privacy settings regularly.
- d) Avoid conduct that may damage professional reputation or public confidence.
- e) Never use social media to discuss confidential school matters.

Any social media activity that affects safeguarding, professional conduct or the reputation of the school may be addressed through school procedures.

## **13. RESPONDING TO ONLINE SAFETY INCIDENTS**

The school will respond promptly and proportionately to online safety concerns.

The school will:

- a) Record significant incidents and actions taken.
- b) Assess risk on a case-by-case basis.
- c) Involve parents and carers where appropriate.
- d) Preserve evidence where possible and appropriate.
- e) Refer concerns to external agencies where necessary.
- f) Provide support for those affected.

Where an incident indicates possible abuse, exploitation or risk of significant harm, it will be managed in accordance with the Child Protection and Safeguarding Policy.

#### **14. MONITORING AND REVIEW**

The effectiveness of this policy will be monitored through:

- Safeguarding audits
- Incident records
- Filtering and monitoring reviews
- Staff feedback
- Governor oversight