St Thomas More Catholic Primary school,
Saffron Walden

ONLINE SAFETY POLICY

Policy No. STM-009

Unique Policy Reference No	***STM-009***
Approved by (inc date)	*Governing Body*
Date Version Approved	*02/04/2025*
Date next due for review	*March 2026*
Author *(Document Owner)*	*Headteacher*

ONLINE SAFETY POLICY

1. INTRODUCTION

1.1. At St Thomas More Catholic Primary School, we are committed to fostering a culture of safeguarding, including online safety, where online harms are not tolerated. We have implemented:

a) A whole-school approach to online safety

b) Training for all staff and visitors in safeguarding and online safety

c) Online safety education within the curriculum

d) Pupil education on technology use and online risks (e.g., online relationships, fake profiles, cyberbullying, online grooming, child sexual exploitation, sexting, live streaming)

e) IT filtering and monitoring systems

f) Awareness of radicalisation through social media

g) Support for victims of online abuse and harassment

1.2. This policy applies to all members of St Thomas More Catholic Primary School who have access to and use school digital technology systems, both on and off-site.

1.3. The **Education and Inspections Act 2006** empowers Headteachers to regulate pupil behaviour beyond school premises, which is particularly relevant to online bullying and other online safety incidents involving school members. The **Education Act 2011** further strengthens these powers concerning the searching of electronic devices and data deletion.

1.4. The school will address such incidents following this policy, the behaviour policy, and the anti-bullying policy. Parents/carers will be informed of any known incidents of inappropriate online behaviour occurring outside of school.

1.5. This policy is reviewed annually by all stakeholders or earlier if required due to technological developments.

2. STATUTORY GUIDANCE AND LEGISLATION

2.1. This policy should be read in conjunction with the following key documents:

a) Keeping Children Safe in Education (2023)

b) St Thomas More Catholic Primary School Child Protection and Safeguarding Policy (2023)

c) Relationships Education, Relationships and Sex Education (RSE) and Health Education (2020)

d) Teaching Online Safety in Schools and Education for a Connected World Framework

e) Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People

f) Harmful Online Challenges and Online Hoaxes (2021)

g) Data Protection Policy

3. ROLES AND RESPONSIBILITIES

3.1. Governors

Governors are responsible for approving and reviewing the effectiveness of this policy through:

a) Regular updates on online safety incidents and monitoring reports

b) A designated Safeguarding Governor who:

   i. Holds meetings with the Designated Safeguarding Lead (DSL)

   ii. Monitors anonymised online safety incidents

   iii. Reviews filtering/change control logs

   iv. Reports to the Governing Body

3.2. Headteacher

The Headteacher has overall responsibility for safeguarding, including online safety, though the day-to-day responsibility is delegated to the DSL.

3.3. Designated Safeguarding Lead (DSL)

The DSL:

a) Leads the development and review of online safety policies

b) Ensures staff are aware of procedures for handling online safety incidents

c) Provides training and advice to staff

d) Liaises with the Local Authority and school technical staff

e) Maintains logs of online safety incidents

f) Regularly meets with the Safeguarding Governor

g) Attends relevant Governors' meetings

h) Reports regularly to the Senior Leadership Team

i) Securing the school’s technical infrastructure

j) Implementing filtering and monitoring systems

k) Keeping up to date with technical developments

l) Monitoring and reporting misuse to the Governors

The DSL must be trained in online safety and aware of safeguarding risks such as:

a) Sharing of personal data

b) Access to illegal/inappropriate materials

c) Inappropriate online contact with adults/strangers

d) Online grooming

e) Cyberbullying

3.4. Teaching and Support Staff

Staff must:

a) Stay informed on online safety policies

b) Sign and adhere to the staff acceptable use policy

c) Report concerns to the Headteacher/DSL

d) Embed online safety in the curriculum

e) Supervise digital technology use in lessons

f) Guide pupils to appropriate online resources

3.5. Pupils

Pupils should:

a) Report abuse, misuse, or inappropriate content

b) Understand and follow policies on mobile devices and digital images

c) Recognise acceptable and unacceptable online behaviour

3.6. Parents/Carers

Parents/carers play a key role in educating children about online safety. The school will provide support through:

a) Newsletters, letters, school website, and social media

b) Parents' evenings and training sessions

c) National online safety campaigns

4. THE CURRICULUM

4.1. The school follows the National Centre for Computing Excellence (NCCE) *Teach Computing* curriculum, covering:

a) Respectful relationships

b) Online relationships

c) Being safe

d) Mental well-being

e) Internet safety and harms

5. EDUCATION AND TRAINING

5.1. Parents/Carers

The school provides guidance through newsletters, parents' evenings, and national campaigns.

5.2. Staff/Volunteers

a) New staff receive online safety training during induction

b) The DSL undergoes regular training updates

c) Online safety updates are provided during staff meetings

5.3. Governors

Governors participate in online safety training through:

a) Local Authority training

b) School-led sessions

6. TECHNICAL INFRASTRUCTURE

The school ensures:

a) Secure networks and access controls

b) Regular security audits

c) Up-to-date virus protection

d) Internet filtering and monitoring to protect against extremist material

7. MOBILE TECHNOLOGIES

7.1. School and personal devices must be used for educational purposes only.

7.2. Safe and appropriate use of mobile technology is embedded in the curriculum.

8. USE OF DIGITAL AND VIDEO IMAGES

8.1. To protect privacy and prevent misuse:

a) Staff educate pupils on safe image sharing

b) Parental consent is required for publishing pupil photos

c) Parents must not share school event images on social media

d) Staff use only school devices for photography

e) Images must respect privacy and dignity

9. DATA PROTECTION

The school complies with the **UK GDPR** and has a **Data Protection Policy**.

10. SOCIAL MEDIA

10.1. School Social Media Accounts

a) Managed by senior leaders

b) At least two staff members oversee administration

c) Clear user behaviour policies and reporting mechanisms

10.2. Staff Use

a) No reference to pupils, parents, or staff on personal social media

b) No discussion of school matters online

c) Security settings must be regularly reviewed

d) Any personal social media use impacting the school falls under this policy

11. MONITORING OF PUBLIC SOCIAL MEDIA

11.1. The school actively monitors social media to protect its reputation and safeguard pupils and staff.

11.2. **Policy Review Date:** Annually or as required due to technological developments.