St Thomas More Catholic Primary School and Nursery
Oxford Road Kidlington OX5 1EA

The Pope Francis Catholic Multi Academy Company

Headteacher: Mrs Julieann Exley

Tel: 01865 373 674 *Email: office@stthomas-more.org.uk* *Website: www.st-thomas-more.oxon.sch.uk*

St Thomas More Catholic Primary School and Nursery

Online Safety Policy

Reviewed by Headteacher & SLT
Review date – September 25
LGB meeting approval - 07.10.25
Review date – September 2026

Chair of The Board of Directors: Mr Paul Concannon

St Thomas More Catholic School and Nursery Online Safety Policy

Introduction

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in Online Safety can mean children are unaware of the unintended consequences of their online behaviour or actions. This highlights the urgent need to educate pupils and the wider school community about both the benefits and risks of using Internet technologies and electronic communications.

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:
Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Legal Framework
This policy outlines our commitment to safeguarding all users and promoting responsible digital citizenship. It provides clear guidance, safeguards, and awareness to enable everyone to control their online experience and manage their digital footprint.

This Online Safety Policy is grounded in the Department for Education's (DfE) statutory safeguarding guidance -
Keeping Children Safe in Education (KCSIE),
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
and incorporates key advice for schools on Teaching Online Safety in Schools,
https://www.gov.uk/government/publications/teaching-online-safety-inschools/teaching-online-safety-in-schools
Preventing and Tackling Bullying and Cyber-bullying,
https://educationhub.blog.gov.uk/2022/11/what-we-are-doing-to-help-combatbullying-in-education
Relationships and Sex Education
https://www.gov.uk/government/publications/relationships-education-relationshipsand-sex-education-rse-and-health-education
Searching, Screening and Confiscation,
https://www.gov.uk/government/publications/searching-screening-and-confiscation

It also draws upon the DfE's guidance on Protecting Children from Radicalisation, https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learnersvulnerable-to-radicalisation
ensuring a comprehensive approach to safeguarding in the digital age.

The policy reflects relevant legislation including the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Equality Act 2010, and the Education Act 2011, which empowers teachers to address cyber-bullying by searching for and deleting inappropriate content on pupils' devices when justified.

Additionally, it aligns with the National Curriculum Computing Programmes of Study, our school's PSHE and RSE curriculum, and national guidance from respected online safety organisations such as National Online Safety, NSPCC, and CEOP.
Our policy and practice against these risks are clearly articulated in this Online Safety Policy.

Our Aims

St Thomas More Catholic Primary School and Nursery is committed to ensuring that we:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (referred to as 'mobile phones' or other 'mobile devices').
- Establish clear mechanisms to identify, intervene, and escalate an incident, where appropriate.

Defining Online Safety

While cybersecurity protects devices and networks from harm by third parties, Online Safety protects the people using them from harm through awareness, education, information, and technology. It is our approach to personal safety when engaging with digital technologies.
Online Safety involves:

- Awareness of potential threats encountered online.
- Protection and management of personal data.
- Online reputation management.
- Avoidance of harmful or illegal content.

It is not about scaremongering or restricting access. Instead, it focuses on the positive and enriching aspects of digital life while recognising its challenges and equipping individuals with the tools to navigate them safely.

Definitions

- Child - on – child sexual abuse and harassment. Pupils may use the internet and technology as a vehicle for sexual abuse and harassment with other pupils.
- Grooming and exploitation. Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/ or abusing them.
- Child sexual exploitation (CSE) and child criminal exploitation (CCE)

    - CSE often involves physical sexual abuse or violence, but online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet.
    - CCE is a form of exploitation in which children are forced or manipulated into crimes for the benefit of their abuser, e.g. drug transportation, shoplifting and serious crime
- Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- Mental Health. The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self- esteem and suicidal thoughts.
- Online hoaxes and harmful online challenges.
    - An online hoax is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or cause distress to individuals, spread through social media platforms.
    - Harmful online challenges refers to challenges that are targeted at young people and generally involves users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same.
- Cyber- crime is criminal activity committed using computers and/ or the internet.

<u>Education and Awareness</u>

We believe that education is the cornerstone of effective online safety. Therefore, we:

- Integrate Online Safety into our curriculum across all key stages.
- Provide regular training and updates for staff, pupils, and parents.
- Promote responsible use of technology through assemblies, workshops, and campaigns.
- Encourage open dialogue about online experiences and concerns.
- Do not allow pupils to bring mobile devices to school.

<u>Roles and Responsibilities</u>

- **Governors**: Ensure strategic oversight and policy compliance. They also ensure that there are appropriate filtering and monitoring systems in place. All governors must complete KCSiE training, Prevent, Cyber bullying, and GDPR training. They should ensure they are aware of online safety issues.
- **Senior Leadership Team**: Lead the implementation and review of the Online Safety Policy. Ensure all staff have completed training for KCSiE, Prevent, Cyber bullying and GDPR training. Inform parents, so that they are aware the issues regarding online safety
- **Designated Safeguarding Lead (DSL):** Coordinate responses to online safety incidents and liaise with external agencies as appropriate.
- **Staff**: Model safe online behaviour and teach about online safety through the curriculum. They have an awareness of online safety issues and can recognise indicators that pupils may be unsafe online and report concerns.
- **Pupils**: Engage responsibly with technology and report anything that makes them feel unsafe.
- **Parents/Carers**: Support the school's approach and reinforce safe practices at home.

Incident Management

We have clear procedures for:

- Monitoring internet use. St Thomas More Catholic Primary School and Nursery uses Securitas to actively monitor internet usage across the school, automatically alerting senior staff to any inappropriate searches or pop-up content to ensure swift safeguarding intervention.
- Reporting online safety concerns, all concerns are logged on CPOMS.
- Investigating incidents promptly and thoroughly.
- Supporting affected individuals.
- Escalating serious cases to appropriate authorities.
- This Online Safety Policy is fully aligned with the statutory guidance set out in Keeping Children Safe in Education (KCSIE), ensuring that all digital safeguarding measures support the broader framework for protecting children from harm.

Policy Review

This policy will be reviewed annually or in response to significant changes in technology, legislation, or school practice.

Linked Policies

- PFMAC – KCSiE
- PFMAC – GDPR policy
- PSHE Policy
- RSE Policy
- Behaviour Policy
- Anti – bullying Policy
- Home/ school Learning Policy/ Pupil Remote learning Policy
- Staff code of Conduct / Acceptable use agreement