



ST THOMAS THE MARTYR CE PRIMARY SCHOOL

IT, COMPUTING AND DIGITAL TECHNOLOGY POLICY

Academic Year: 2026–2027

Review Date: September 2027

Approved by: Governing Body

Policy Lead: Headteacher – Mr C Roscoe/ Computing Lead – Mrs. M Mason

Date Approved: 01.09.26

“May all that we do be done with love.”

1. Introduction

At St Thomas the Martyr CE Primary School, we recognise that information technology, computing and digital technology are an essential part of modern life and an important component of a broad and balanced education.

Technology provides powerful opportunities for teaching, learning, communication, creativity and collaboration. We want our pupils to become confident, capable and responsible users of technology who understand both its benefits and its potential risks.

Our approach to IT and digital technology is underpinned by our Christian vision and commitment to ensuring that technology is used respectfully, safely, responsibly and with love for others.

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Acceptable Use Policy
- Behaviour Policy
- Data Protection and Privacy Policy
- Cyber Security arrangements
- Staff Code of Conduct
- Mobile Phone Policy
- Remote Education arrangements
- SEND Policy
- Curriculum Policy

2. Aims

The school aims to:

1. Provide pupils with high-quality opportunities to develop digital and computing knowledge and skills.
2. Enable pupils to use technology creatively, confidently and safely.



3. Develop pupils' understanding of computer science, information technology and digital literacy.
 4. Teach pupils how to recognise and manage online risks.
 5. Promote responsible, respectful and ethical behaviour when using technology.
 6. Ensure that technology supports high-quality teaching and learning across the curriculum.
 7. Provide equitable access to appropriate digital resources.
 8. Protect pupils, staff and visitors from inappropriate or harmful online content.
 9. Maintain appropriate filtering and monitoring arrangements.
 10. Protect personal and school data.
 11. Develop staff confidence and competence in using digital technologies.
 12. Encourage pupils to become discerning consumers and creators of digital content.
 13. Prepare pupils for the continuing development of technology, including artificial intelligence.
-

3. Curriculum

Computing is taught as a discrete subject and is also used meaningfully across the wider curriculum.

The computing curriculum incorporates three key areas:

Computer Science

Pupils develop an understanding of:

- algorithms
- programming
- computational thinking
- logical reasoning
- debugging
- how digital systems work
- networks and communication.

Information Technology

Pupils learn to:

- create, organise and manipulate digital content
- use word processing and presentation software
- work with data
- use multimedia
- communicate using appropriate digital tools
- select appropriate technology for particular purposes.

Digital Literacy

Pupils learn how to:

- use technology safely
- recognise inappropriate content
- understand online relationships



- protect personal information
 - recognise online risks
 - respond appropriately to cyberbullying
 - understand the impact of their digital footprint
 - evaluate the reliability of online information
 - behave respectfully online.
-

4. Digital Technology Across the Curriculum

Technology should enhance learning rather than replace effective teaching.

Staff are encouraged to use digital technology where it:

- improves access to learning
- supports individual needs
- increases engagement
- enables collaboration
- provides opportunities that would otherwise be unavailable
- develops digital skills
- supports assessment
- enables pupils to communicate and present their learning.

Technology may be used across subjects including English, mathematics, science, history, geography, art, music, PE, RE and PSHE.

5. Online Safety

Online safety is an integral part of safeguarding at St Thomas the Martyr CE Primary School.

Pupils are taught about the potential risks associated with technology, including:

- inappropriate content
- online bullying
- grooming
- exploitation
- inappropriate communication
- sharing personal information
- excessive or inappropriate use of technology
- misinformation and disinformation
- scams and fraud
- gaming risks
- online relationships
- artificial intelligence
- image manipulation and deepfakes



- digital footprints
- inappropriate use of photographs and videos.

Pupils are taught to **STOP, BLOCK and TELL** when they encounter something online that makes them feel uncomfortable, worried or unsafe.

All online safety concerns must be reported in accordance with the school's safeguarding procedures.

KCSIE 2026 makes clear that safeguarding includes recognising and responding to online harms, and that staff must act promptly when concerns arise.

6. Filtering and Monitoring

The school will maintain appropriate filtering and monitoring systems to protect pupils and staff from illegal, inappropriate and potentially harmful content.

Filtering is preventative and aims to restrict access to inappropriate content. Monitoring is reactive and enables the school to identify potentially concerning activity.

The school will:

- maintain appropriate filtering systems;
- maintain appropriate monitoring systems;
- regularly review the effectiveness of filtering and monitoring;
- ensure that pupils and staff are identifiable when using school systems where reasonably possible;
- investigate safeguarding alerts;
- record significant incidents and actions;
- ensure that the DSL and IT support work together;
- ensure governors receive appropriate assurance regarding filtering and monitoring;
- review provision at least annually;
- respond to identified weaknesses promptly.

The school recognises that no filtering system is completely effective. Staff must therefore provide appropriate supervision and pupils must receive regular online safety education.

The DfE requires schools to have effective filtering and monitoring arrangements and recommends an annual review involving senior leaders, the DSL, IT support and the responsible governor.

7. Roles and Responsibilities

Governing Body

Governors will:

- provide strategic oversight of digital technology;
- ensure appropriate safeguarding arrangements are in place;



- receive assurance regarding filtering and monitoring;
- ensure significant risks are identified and addressed;
- monitor the effectiveness of the school's IT provision;
- ensure appropriate resources are available;
- review relevant policies.

Headteacher

The Headteacher will:

- have overall responsibility for implementation of this policy;
- ensure that IT contributes to school improvement;
- ensure staff understand their responsibilities;
- work with the DSL and IT support regarding online safety;
- ensure significant incidents are appropriately managed.

Designated Safeguarding Lead

The DSL will:

- lead on safeguarding concerns arising from technology use;
- respond to filtering and monitoring alerts where appropriate;
- ensure concerns are recorded and acted upon;
- ensure online safety forms part of safeguarding education;
- work closely with IT support and senior leaders.

Computing / IT Lead

The Computing / IT Lead will:

- coordinate the computing curriculum;
- support staff development;
- monitor standards in computing;
- advise on digital resources;
- support effective use of technology;
- contribute to online safety education;
- work with IT providers where appropriate.

IT Support / Provider

IT support will:

- maintain devices and systems;
- maintain filtering and monitoring arrangements;
- support cyber security;
- investigate technical issues;
- provide relevant reports;
- escalate safeguarding concerns to the DSL;
- maintain appropriate system security.



All Staff

All staff must:

- follow the school's IT and acceptable use policies;
 - use technology appropriately;
 - protect passwords and accounts;
 - report concerns promptly;
 - maintain professional boundaries online;
 - supervise pupils appropriately;
 - use only approved systems and applications;
 - protect personal and confidential information.
-

8. Acceptable Use – Pupils

Pupils must:

- use school devices for appropriate educational purposes;
- follow instructions from staff;
- use respectful language;
- keep passwords confidential;
- report anything worrying or inappropriate;
- use only their own accounts;
- respect other people's files and information;
- follow copyright and intellectual property rules;
- take care of school equipment.

Pupils must not:

- deliberately access inappropriate material;
 - attempt to bypass school filtering;
 - share passwords;
 - access another person's account;
 - download unauthorised software;
 - use technology to bully, threaten or upset another person;
 - take photographs or recordings without permission;
 - share personal information inappropriately;
 - use another person's identity;
 - deliberately damage equipment or systems.
-

9. Acceptable Use – Staff

Staff must use school technology professionally and responsibly.



Staff must:

- use approved school systems;
- maintain professional boundaries;
- protect passwords;
- lock devices when unattended;
- report lost or stolen equipment;
- report suspected cyber incidents;
- protect confidential information;
- use appropriate professional communication;
- follow the school's safeguarding procedures.

Staff must not:

- use personal email accounts for confidential school business;
 - share confidential information through unauthorised services;
 - communicate with pupils through personal social media accounts;
 - use personal devices to store confidential pupil information unless explicitly authorised;
 - access inappropriate material;
 - disable or circumvent security measures.
-

10. Passwords and Account Security

Users must:

- maintain strong passwords;
- never share passwords;
- avoid using easily guessed passwords;
- use multi-factor authentication where provided;
- log out when appropriate;
- report suspected compromised accounts immediately.

Staff should never write passwords where pupils or unauthorised persons can access them.

11. Data Protection

The school will process personal data in accordance with applicable data protection legislation and DfE guidance.

Personal data must only be:

- collected when necessary;
- accessed by authorised individuals;
- stored securely;
- shared appropriately;



- retained for appropriate periods;
- disposed of securely.

Staff must take particular care with:

- pupil records;
- safeguarding information;
- photographs;
- medical information;
- SEND information;
- contact details;
- assessment information;
- staff information.

The DfE's current school data protection guidance was updated in July 2026, including changes relating to the Data (Use and Access) Act 2025 and educational technology.

12. Artificial Intelligence

The school recognises that generative artificial intelligence is increasingly being used in education.

AI tools may only be used where:

- they have been appropriately assessed;
- they are suitable for the age of pupils;
- their use complies with data protection requirements;
- staff understand the limitations and risks;
- their use supports, rather than replaces, professional judgement.

Staff must not enter confidential or identifiable pupil information into an AI system unless the system has been formally approved for that purpose.

Pupils will be taught that AI-generated information may be inaccurate, biased or misleading.

The school will promote responsible use of AI, including:

- checking information;
- identifying AI-generated content;
- understanding bias;
- protecting personal information;
- respecting copyright;
- understanding academic honesty;
- recognising manipulated images, audio and video.

The DfE's digital standards were updated in August 2026 to address risks associated with generative AI products.



13. Mobile Phones and Smart Devices

The school's approach to mobile phones and smart technology will comply with current statutory guidance.

From September 2026, schools are expected to follow statutory guidance requiring policies that prohibit pupil mobile phone use throughout the school day, including lessons, breaktimes and lunchtimes, subject to appropriate school arrangements and exceptions.

St Thomas the Martyr CE Primary School will therefore maintain clear expectations regarding:

- mobile phones;
- smart watches;
- tablets;
- cameras;
- wearable technology;
- other internet-connected personal devices.

Any permitted exceptions will be determined by the Headteacher in accordance with safeguarding, medical or individual needs.

14. Photography and Video

Photographs and videos involving pupils must be taken and used in accordance with:

- parental consent arrangements;
- safeguarding procedures;
- data protection requirements;
- school policy.

Staff must only use approved school equipment and systems unless specific permission has been granted.

Images must not be shared through personal social media accounts.

15. Cyber Security

The school will take reasonable and proportionate steps to protect its systems from cyber threats.

This includes:

- secure passwords;
- appropriate access controls;
- software updates;
- anti-malware protection;
- secure networks;



- backups;
- staff awareness;
- incident reporting;
- appropriate device management.

Staff must report suspected phishing emails, malware, lost devices, suspicious activity or compromised accounts immediately.

16. Remote Learning

Where remote learning is required, the same safeguarding and professional expectations apply as in school.

Staff must:

- use approved platforms;
- maintain professional boundaries;
- follow safeguarding procedures;
- avoid sharing personal contact details;
- ensure online teaching is appropriately supervised;
- record and report safeguarding concerns.

The DfE states that safeguarding principles continue to apply when education is delivered remotely.

17. Inclusion and Accessibility

The school will seek to ensure that technology supports all pupils, including pupils with SEND.

Appropriate technology may include:

- accessibility tools;
- text-to-speech;
- speech-to-text;
- visual supports;
- adapted keyboards and mice;
- communication technology;
- assistive software.

Technology will be selected according to individual needs and educational benefit.

18. Equipment

Pupils and staff are expected to take reasonable care of school technology.



This includes:

- computers;
- laptops;
- tablets;
- interactive displays;
- cameras;
- printers;
- networking equipment;
- charging equipment;
- other digital resources.

Damage caused deliberately or through inappropriate use will be investigated in accordance with the school's behaviour and disciplinary procedures.

19. Internet and Email

School internet and email systems are provided primarily for educational and professional purposes.

Users must:

- communicate respectfully;
- avoid inappropriate content;
- avoid opening suspicious attachments;
- check recipients carefully;
- protect confidential information;
- report suspicious messages.

School email accounts must not be used to create inappropriate online accounts or for unauthorised commercial activity.

20. Social Media

Staff must maintain appropriate professional boundaries online.

Staff should not:

- communicate with pupils through personal social media accounts;
- post confidential school information;
- publish inappropriate images involving pupils;
- identify pupils without appropriate permission;
- make comments that could damage the reputation of the school.

The school recognises that online conduct outside school can affect safeguarding, professional relationships and the reputation of the school.



21. Copyright and Intellectual Property

Staff and pupils should respect copyright and intellectual property rights.

Digital resources should be used in accordance with relevant licences and permissions.

Pupils should be taught to:

- acknowledge sources;
 - avoid plagiarism;
 - understand copyright;
 - use images and media responsibly;
 - distinguish between their own work and material generated or sourced elsewhere.
-

22. Incident Management

Any suspected IT or online safety incident must be reported promptly.

Examples include:

- inappropriate websites;
- cyberbullying;
- hacking attempts;
- phishing;
- malware;
- loss of equipment;
- inappropriate messages;
- compromised accounts;
- accidental disclosure of personal information;
- deliberate attempts to bypass filtering.

The school will investigate incidents proportionately and may involve:

- the Headteacher;
- DSL;
- Computing / IT Lead;
- IT provider;
- parents/carers;
- governors;
- external agencies;
- police or other safeguarding partners where appropriate.

Safeguarding concerns must be managed in accordance with the Child Protection and Safeguarding Policy.



23. Monitoring and Evaluation

The effectiveness of this policy will be monitored through:

- filtering and monitoring reports;
- safeguarding records;
- online safety incidents;
- pupil voice;
- staff feedback;
- parental feedback;
- curriculum monitoring;
- governor monitoring;
- annual filtering and monitoring review;
- IT security reviews;
- assessment of computing outcomes.

Findings will inform school improvement planning and staff training.

24. Training

All staff will receive appropriate training regarding:

- online safety;
- safeguarding and online harms;
- acceptable use;
- data protection;
- cyber security;
- filtering and monitoring;
- safe use of digital platforms;
- artificial intelligence where relevant.

New staff will receive appropriate information during induction.

KCSIE 2026 requires staff to understand their safeguarding responsibilities, including online harms, and to follow school safeguarding procedures.

25. Parents and Carers

The school will work with parents and carers to promote safe and responsible technology use.

Parents and carers will be provided with appropriate advice and information regarding:

- online safety;



- gaming;
- social media;
- parental controls;
- age restrictions;
- mobile phones;
- online bullying;
- privacy;
- emerging technologies.

Concerns involving online activity outside school may be considered where they affect pupil welfare, safeguarding or the school community.

26. Governors' Assurance

The governing body will receive appropriate assurance that:

- filtering and monitoring are operational;
- the annual review has been completed;
- identified risks are being addressed;
- staff have received appropriate training;
- safeguarding concerns are managed effectively;
- cyber security arrangements are appropriate;
- technology supports school improvement;
- relevant policies remain current.

The DfE expects governors/proprietors to have appropriate oversight of filtering and monitoring and to ensure that provision is reviewed regularly.

27. Review

This policy will be reviewed annually or sooner where there are:

- significant changes to legislation;
- changes to DfE guidance;
- significant technological developments;
- changes to school systems;
- significant safeguarding incidents;
- recommendations arising from monitoring or review.

Next review: September 2027



Appendix 1 – Pupil Digital Safety Rules

SMART

S – Stay safe

Keep personal information private.

M – Make good choices

Use technology responsibly.

A – Ask for help

Tell an adult if something worries you.

R – Respect others

Be kind online and offline.

T – Think before you click

Check links, messages and information before acting.

Appendix 2 – Staff Digital Safety Checklist

Staff should ask:

- Am I using an approved system?
 - Am I protecting personal information?
 - Would I be comfortable for this communication to be reviewed?
 - Have I maintained professional boundaries?
 - Is this resource appropriate for the age of the pupils?
 - Have I considered online safety?
 - Have I checked the accuracy of digital or AI-generated information?
 - Have I reported any safeguarding or cyber security concern?
-

Appendix 3 – Key Documents and Guidance

This policy should be implemented alongside the current versions of relevant DfE guidance, including:

- Keeping Children Safe in Education 2026
- Meeting Digital and Technology Standards in Schools and Colleges
- Data Protection in Schools
- Mobile Phones in Schools
- relevant safeguarding, data protection and cyber security guidance.

Policy status: To be approved

Chair of Governors: S Osmond_____

Headteacher: C Roscoe_____

Date: 01.09.26_____