St Thomas More Primary School

Online Safety Policy

Updated by: C. Sharp / L. Coleman

Date: September 2025

Review Date: September 2027

The subject of Computing is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at St Thomas More we need to build in the safe and responsible use of digital technologies, in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making the best use of technology, information, training, and this policy, to create and maintain a safe digital environment for our school.

Roles and Responsibilities

Governors:

- Ensure an appropriate senior member of staff is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status and authority and time, funding, training, resources and support.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Sign and follow the Acceptable Use policy and code of conduct (Appendix A).

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and deputy headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The ICT Co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.

All Staff (Including Student teachers):

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know who the Designated Safeguarding Leads are (S. Hewitt, M. Allcock and G. Postles).
- Read and follow this policy in conjunction with the school's main Safeguarding Policy.
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the Staff Acceptable Use policy and code of conduct (Appendix A).
- Sign and follow the Device Usage Policy (Appendix B).
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.

- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Prepare and check all online source and resources before using within the classroom.
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Volunteers and Contractors:
- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

Pupils:
- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually (KS1 - Appendix C, KS2 - Appendix D).
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Teaching and Learning

The Internet:
- The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:
- The school Internet access will be designed expressly for pupil use including appropriate content filtering. Internet usage is monitored by Headteacher and IT co-ordinator.

- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new Computing curriculum, all year groups have digital literacy objectives that focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

Google Classroom:

- Google's Privacy Policy for GSuite can be found here: https://policies.google.com/privacy/update

- When using the livestream function:
  - Only use school-registered accounts, never personal ones - this applies to staff and teachers.
  - Keep a log of livestreams - what, when, with whom and record anything that went wrong.
  - Students should not share any meeting links with anyone.
  - A minimum of 3 people on the call, to avoid 1 to 1 – the teacher may terminate the call.
  - Do not share any personal information during the call.
  - Behaviour is to be of a high standard in order to allow all students to learn, anyone not upholding to these standards will be muted and removed for the call and parents will be informed.
  - If camera is on – participants must be dressed appropriately and are not allowed to attend meetings in their pyjamas.
  - Think about the background and privacy of others who may come into view in the camera - use of blurred background is advised.

  Please see separate DPIA Policy for Data protection risks and procedures relating to Google Classroom.

Authorised Internet Access

- By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use.
- All staff must read and sign the 'Acceptable Use Agreement' before using any digital school resource.
- Only authorised equipment, software and Internet access can be used within the school.

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- E-mail sent to external organisations should be written carefully and in line with current GDPR guidelines.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

- GDPR guidelines must be followed to ensure all data and information is sent in a secure manner via email.
- If an email is being sent to multiple people outside of the school staff then BC must be used accordingly.

Security and passwords:
- Passwords should be changed regularly. The system will inform users when the password is to be changed.
- Pupils and staff should never share passwords and staff must never let pupils use a staff logon under any circumstances.
- Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking:
- Social networking Internet sites (such as Twitter, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups, in the school, is not allowed and will be blocked/ filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised of age limits that are set for the different social network platforms.
- Pupils will be encouraged to only interact with known friends, family over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.
- The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting:
- Incidents which may lead to a child protection issue needs to be passed onto Mrs Hewitt, Mrs Allcock or Mr Postles **immediately**.
- Incidents which are not child protection issues but may require SLT intervention (e.g. cyberbullying) should be reported to SLT in the same day.
- Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.
- Evidence of incidents must be preserved and retained.
- The curriculum will cover how pupils should report online incidents, both in and outside of school, (e.g. Ceop button, trusted adult, Childline)

Mobile Phones:
- There are risks of mobile bullying, or inappropriate contact.
- Pupils, by permission of the Headteacher, can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.

- Staff should always use the school phone to contact parents.
- Staff, including student teachers, and visitors are not permitted to access or use their mobile phones within the classroom when children are present. If a child can be seen then their mobile phone should not be.
- All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff members or parents cannot use mobile phones on school trips to take pictures of the children. This should be done using the teacher's school ipad.
- On trips, staff mobiles are used for emergency only.

Digital/Video Cameras/Photographs:
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- Staff should always use a school camera to capture images and should never use their personal devices.
- Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website
- The school website is a valuable source of information for parents and potential parents.
- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- Mrs Hewitt and Mrs Tonks will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.
-

Information System Security
- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly - teachers to ensure school issued laptops are brought in to school at least once a week and turned on to run relevant updates.
- Security strategies will be discussed with the Local Authority.

<u>Communication of Policy</u>

Pupils:
- Rules for Internet access will be posted in all rooms.
- Pupils will be informed that Internet use will be monitored.

- Pupils will be informed of the importance of being safe on social networking sites such as msn. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.
- Pupils will be asked to sign an age appropriate User Agreement Policy (UAP).

Staff:
- All staff will be given the School e-safety Policy and its importance explained.
- Staff and Governors will be asked to read and sign a UAP.
- Staff are asked to accept an electronic version of the UAP every time they log into the school system.

Parents:
- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.
- E-safety workshops will be held to inform parents of the importance of e-safety.

Approved by:

IT Co-ordicator: Date:

Headteacher: Date:

Governors: Date:

Appendix A: Staff and Governor User Agreement Policy

St Thomas More Primary School

Acceptable Use Agreement - Staff and Governors

Background and purpose

Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements. The school's internet, network and ICT systems and subscriptions to services should be used appropriately at all times.

The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

• I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.

• I will educate children in my care about the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.

• I understand my use of the school's ICT systems/networks and internet are monitored.

• I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.

• I know what GDPR is and how this has a bearing on how I access, share, store and create data.

• Any data that I have access to away from school premises must be kept secure and used with specific purpose.

• I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.

• I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.

• If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me (outlined in the Social Media Policy), with particular care given to what images/video imagery and details can be uploaded.

• I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts.

• I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviour/conduct, I will notify the school at the earliest opportunity.

• I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.

• I will never download or install software unless permission has been given by the appropriate contact at school.

• I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy.

• I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely.

• Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.

• I understand that mobile devices, including smart watches, shall not be used, nor in my possession, during times of contact with children. These devices will be securely locked away with adequate password protection on them should they be accessed by an unauthorised person.

• Any school trips/outings or activities that require a mobile phone/ camera I will abide guidelines set out in the school's Mobile Phone Policy.

• At no point- will I use my own devices for capturing images/ video or making contact with parents/carers.

Staff Name:

Signature:

Date:

Appendix B: Device Usage Policy

St Thomas More Primary School

Device Usage Policy

Created: **October 2020**

Reviewed: September 2025

What Is the Policy?
The policy outlines the responsibilities that St Thomas More Primary School staff must accept when they are issued with a laptop or any other electronic device such as an iPad, camera, Mobile phone or Chromebook.

Who Is Affected By The Policy?
This policy applies to members of staff within St Thomas More Primary School who have been issued with an electronic device.

Why Was This Policy Created?
Laptops and iPads provide the convenience of portability. This convenience exposes the school to certain risks. These include, but are not limited to:

- Theft of school property – laptops and iPads are easy to steal and their relatively high value and easiness to sell makes them common targets of theft.
- Exposure of sensitive data or information – misplaced or unsecured laptops may expose sensitive information to the public. Loss of such data could be utilised by sections of the public for illegal purposes.
- Damage of school property – Laptops and iPads can be susceptible to damage both due to their nature and their relatively fragile construction.

Any member of staff issued with a laptop or an iPad will need to confirm, by signing an acceptance of this policy, that he/she has read, understands and will comply with the policy.

The policy will need to be signed by the member of staff, with a copy kept in the school office until the laptop or iPad is returned or replaced.

A copy of the policy is available from the school's Office Manager.

Content
When a St Thomas More Primary School employee is provided with a laptop or iPad, he/she accepts responsibility for safeguarding the device itself as well as the data stored on it.

Staff users are expected to exercise reasonable care and take the following precautions:-

- Ensure they have appropriate car and house insurance to be able to transport/use the laptop on St Thomas More Primary School business.
- Take appropriate steps to protect the laptop from theft:
    1. Staff should make every reasonable effort to keep their laptop safe overnight.
    2. Laptops, where possible, should not be left unattended in a parked car. On those occasions where there is no alternative, they should be locked in the boot.
- Do not work or save sensitive information on a laptop without taking the appropriate precautions:-
    1. Sensitive information refers to any data that is protected by the school's policy, or by any local or national laws or regulations. This includes but is not limited to; education records, personally identifiable information and confidential internal school information.
- All members of staff are accountable for all network and systems access under their user ID, so passwords should be kept absolutely secret. It should never be shared with anyone, especially not a pupil.

- School laptops are provided for official use by authorised employees. St Thomas More Primary School devices must not be loaned or be allowed to be used by others.
- Avoid leaving your laptop unattended and logged on. Always shut down, log off or lock the screen before walking away from the machine.
- Members of staff should only use their school G-Suit account to log into Google on their school issued devices.

Take Care to Protect the Laptop from Damage

- Laptops should not be used in environments that might increase the likelihood of damage.
- When taking laptops off site they should be carried and stored in a padded laptop computer bag to reduce the risk of accidental damage.

Virus Protection

- Viruses are a major threat to the school and laptops are particularly vulnerable if their anti-virus software is not kept up to date. The anti-virus software must be updated weekly. The easiest way to do this is to log onto the school network with your device for the automatic process to run.
- E-mail attachments are one of the main sources of computer viruses. Avoid opening any e-mail attachments unless they are expected from a legitimate source.
- Report any security incidents (such as virus infections) promptly to the IT co-ordinator and headteacher in order to minimise the risk of damage.

Software Installations

- Do not download, install or use any unauthorised software programs.
- Any software that is required to be installed must be installed through the IT co-ordinator who will liaise with Entrust. He/She will need to have proof of license and will store the license securely for audit purposes.

Inappropriate Materials

- St Thomas More Primary School will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop or iPad and steer clear of dubious websites.

Report Damage or Loss As Soon As Possible

- Any damage or loss must be reported immediately to the headteacher.

Upon the end or termination of your employment, the device must be returned to the headteacher.

St Thomas More Primary School Laptop Usage Policy

I can confirm that I have read, understood and will comply with the above mentioned policy.

Name……
(In block capitals please)

Signed ……..

Date …….

Appendix C: KS1 User Agreement Policy

KS1 Acceptable Use Agreement

- I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite when I post to use our email and other communication tools.
- I understand this agreement and know the consequences if I don't follow it.

Class Name:

Date;

Children's names;

Appendix D: KS2 User Agreement Policy

KS2 Acceptable Use Agreement

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.

- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.
    - **T** - it is True?
    - **H** - is it Helpful?
    - **I** - is it Inspiring?
    - **N** - it is Necessary?
    - **K** - is it kind?

I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

Name:

Date: