believe to achieve

St. Thomas' CE Primary School

E-Safety & Child Friendly Policy

Written by Megan Finlayson	March 2026
Approved by Governors	16th March 2026
Review Date	March 2028

This Online Safety Policy outlines the commitment of St Thomas' CE Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

St Thomas' CE Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Why is the internet important?

Computing and E-safety is a crucial component of children's life and education in today's ever-growing digital world and is ingrained in our school's computer curriculum due to the current increase in technology usage.

The Internet and other digital and information technologies are effective instruments that open up new opportunities for everyone. Electronic communication makes it more effective for students and teachers to share knowledge. These technological advancements can encourage conversation, encourage creativity, and heighten contextual awareness to support effective learning. Children and young people should have an entitlement to safe internet access at all times.

At School

At St Thomas', we believe it is crucial to help both parents and children truly understand E-safety problems so they may learn how to use the internet and other digital media safely and securely as well as how to support one another when doing so.

We strongly believe that the use of the Internet and online communication is hugely worthwhile and an essential learning tool for our pupils as they grow up in the modern world. However, there are always concerns about children having access to undesirable materials and at school we have taken positive steps to deal with this risk in school. Our school internet access provider operates the Smoothwall filtering system that restricts access to inappropriate materials. Children are also educated through the Computing curriculum on how to report any inappropriate material. All children in school are encouraged to apply their learning into their everyday lives.

As part of the wider curriculum, access to the internet is given to the children in teacher supervised lessons and is strictly monitored by the senior leadership team.

At St Thomas', we have our Digital Leaders to help support other students and teachers with the technology around school, as well as promoting E-safety when necessary.

Pupils will be taught how to evaluate Internet content and the school ensures that the use of Internet derived materials by staff and by pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy as part of our 'SMART' e-safety digital literacy teaching.

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

Headteacher and Senior Leaders:

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1].
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- 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 online safety monitoring role.
- The Headteacher & Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles.
- The Senior Leadership Team will undertake regular monitoring of E-safety and report to staff & Governors.

Teaching and support staff
Teaching and Support Staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood, and signed the staff acceptable use agreement (AUA)
- They immediately report any suspected misuse or problem to *(insert relevant person)* for investigation/action, in line with the school safeguarding procedures
- All digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

The expectations of internet use within school
Just as they are expected to behave everywhere else in school, we expect staff and children to be accountable for their actions while using the internet. Before using the Internet, students should always ask permission and have a clear purpose in mind. Personal information, such as home addresses and phone numbers will not be revealed by children and staff on the web or in dialogue with other internet users.

Children are only permitted to use email under supervision and if part of a lesson. All email will be moderated and monitored by the class teacher. Children will not engage in any form of conversation or dialogue with other users on the Internet in school without permission and supervision from their teacher. The use of public chat rooms and Internet Messaging Services is prohibited. The use of social networking sites such as Facebook are not generally appropriate to primary education and the use of the Internet for such purposes is not currently permitted. Computers should only be used for schoolwork and homework.

Only staff and children under adult supervision are allowed to download files. Students using the Internet are to refrain from purposefully looking for offensive content. Should any child unintentionally come across such information, or if they feel uncomfortable or distressed by anything they find online, they will immediately switch off the monitor and report it to the adult in charge. Any adult in the child's care should immediately notify the head teacher, and this will be investigated further using the correct procedure.

Child Friendly Policy

1) Don't post any personal information online – like your address, email address or mobile number
2) Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online, most people can see it and may be able to download it, it's not just yours anymore
3) Keep your privacy settings as high as possible
4) Never give out your passwords
5) Don't befriend people you don't know
6) Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do
7) Remember, that not everyone online is who they say they are
8) Think carefully about what you say before you post something online
9) Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude
10) If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately

Published content

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils personal information will not be published on the website or on class DOJO.

- The Headteacher will take overall editorial responsibility to ensure that content is accurate and appropriate.
- Parents complete a permission form at the start of enrolment which is updated regularly throughout the child's time at the school. This permission form states whether the parent allows their child to be on school media platforms. This information then gets passed on to all staff in the school.

Parents and carers

Parents and carers play an important role in ensuring that their children understand the need to use the internet or mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, websites and information about national, local E-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Digital media on class DOJO
- Digital media on the school website
- Digital media on Twitter

Appendix A - Internet Safety and the use of Social Media – Year 5 & 6

Dear Parent/Carer,

Internet safety and the use of Social Media – Year 5 & 6

St Thomas' CE Primary School is committed to promoting the safe and responsible use of the internet and as such we feel it is our responsibility to raise this particular issue, due to the increase in inappropriate use of Skype, Snapchat, Instagram, Facebook, YouTube and group games such as Fortnite and Tiktok. Many of the issues that have been brought to our attention recently have involved the use of these sites even though the majority of them have an age restriction which is above a Primary School aged child.

We understand that it is increasingly difficult to keep up with the ways that our children are using new and ever changing technologies. Our children are immersed in a society that has become dependent on powerful computers, including smart phones, iPads, interactive online games and virtual communities.

Websites such as Facebook, Instagram, X, YouTube and WhatsApp to name but a few, offer fantastic opportunities for communication and social connections, however they are created with their audience in mind especially sites such as Facebook and Instagram which are specifically for those over 13 years old. When monitoring your son/daughter's internet use, please remind yourself of the concerns of social media:

- Many sites use 'targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated when they registered. They may have lied about their age to get an account, making them appear older than they are, increasing this risk.
- Young people may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour. The general rule is, if they aren't friends in real life, they shouldn't be 'friends' online
- Language, games, groups and content posted or shared on social media is NOT moderated, and therefore can be offensive, illegal or unsuitable for young people
- Photographs shared by users are NOT moderated and therefore young people could be exposed to inappropriate images or even post their own
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and options
- Social media sites can be exploited by bullies and for inappropriate contact
- Social media sites cannot and do not verify its members, therefore, it is important to remember that if your son/daughter can lie about who they are online, so can anyone else

Primarily, these occurrences and reported incidents of misuse of social media sites happen at home, after school hours when children have access to web sites that are blocked in school. With this in mind, and in response to concerned parents who have asked for advice regarding internet safety, we feel it important to point out to parents the risks of unregulated use of such sites, so you can make informed decisions as to whether to allow your child to have a profile or not and when and how to monitor their use, particularly at night time. We strongly advise a device free bedroom policy after bedtime to allow for uninterrupted sleep and rest.

Although we cannot govern matters occurring out of school hours which is parental responsibility, we will take action (such as reporting under age profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our pupils, including reporting the use of in appropriate images of young people to the police, as this is a legal matter. This also refers to inappropriate text messages.

Should you decide to allow your child to have an online profile we strongly advise you:

- Check their profile is set to private and that only their friends can see information they post
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting or messaging offensive /inappropriate messages or photos
- Monitor your child's use of language and how they communicate to other people, ensuring profanity is discouraged
- Have a look at advice for parents on the social media sites
- Set up your own profiles so you understand how the site works and ask them to have you as their friend on their profile so you know what they are posting online

Make sure your son/daughter understand the following rules:

- Always keep your profile private
- Never accept friend you do not know in real life
- Never post anything which could reveal your identity including photographs wearing school uniform where possible
- Never post anything you wouldn't want your parents or teachers to see
- Never agree to meet somebody you only know online without telling a trusted adult
- Always tell someone if you feel threatened or someone upsets you

We recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online:
www.thinkuknow.co.uk
www.net-aware.org.uk
www.getsafeonline.org

Through lessons provided at school, assemblies, guest speakers, and PSHE lessons, we do our best to provide our children with the awareness and knowledge they need in order to recognise and avoid dangerous, destructive, or unlawful behaviour and to respond appropriately. However, it is only through a collaborative effort between parents and teachers that we will succeed in creating responsible and safe cyber citizens.