E-Safety Policy

If you require this document in an alternative format please contact
office@tssmat.staffs.sch.uk or 01543 472245

Last review date:		May 2023		
Next Review date:		May 2024		
Review Cycle:		Annually		
Statutory Policy:		Yes		
Publication:		Website. G/Policies		
Owner		J Wynn		
Date	**Version**	**Reason for change**	**Overview of Changes made**	**Source**
21.05.20	1.0	Scheduled Revision	Ratified	SCC
13.05.21	1.1	Scheduled Internal Lead Review	Update to logo and name.	
09.07.21	1.2	Scheduled Board Lead Review	No changes. SLT	
09.07.21	2.0	Scheduled Board review	Ratified	
13.03.22	2.1	Scheduled Internal Lead Review	No changes. J Wynn	
07.04.22	2.2	Scheduled Board Lead Review	No changes. H Bowman	
17.06.22	3.0	Scheduled Board review	Ratified	
28.03.23	3.1	Scheduled Internal Lead Review	No changes. J Wynn	
25.04.23	3.2	Scheduled Board Lead Review	No changes. H Bowman	
05.05.23	4.0	Scheduled Board review	Ratified	

E-Safety Policy

Summary

The E-Safety Policy is part of School Development Plans, and relates to other policies including those for computing, bullying and child protection. As such, it will be reviewed annually in light of changes to school and technology.

The Trust has an e-Safety Coordinator, currently the Computing subject lead. This coordinator works in conjunction with the CEO, and the designated Director for e-safety. As such, a whole Trust approach is ensured.

To enable community links to be fostered and developed with regards to wider safety aspects, a working party comprising parents, children and interested parties from the community will be established to ensure holistic impact.

The Trust network is monitored by Senso software which flags up inappropriate content. The software reports incidents which are checked by the School Secretary on a regular basis, and if required these are reported to the e-Safety Co-ordinator or Headteacher.

Teaching and learning

The Internet is an essential element in 21st century life for education, business and social interaction. The Trust has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The Trust Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They are also taught the importance of cross-checking information before accepting its accuracy and how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

The Trust will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Trust ICT systems security will be reviewed regularly, virus protection will be updated regularly and security strategies will be discussed with the IT Provider when appropriate

Staff use a Trust phone when contact with pupils is required. Personal mobile phones shall never be used to capture photographs of pupils. School cameras and secure iPads are used. See our Use of Photographs and Images Policy, Pupil Privacy Notices, and Retention Schedule for more details on how these are used and stored.

Protecting children

We have put in place the following safeguards to keep children safe whilst accessing the internet on the Trust's computers:

- A risk assessment has been undertaken.
- Parental controls have been activated on all computers accessible to children:
    - Google SafeSearch Filtering is turned on
    - YouTube Restricted Mode is set to on
    - Senso is turned on
- The computers are located so that the screens can easily be seen from the rest of the room.
- Staff closely monitor children and the sites that they are accessing when they use the internet.
- The computers have an up to date virus checker and firewall installed.
- The computers' browser histories are regularly checked to monitor which sites are being accessed. All staff and children are informed of this fact.

Email

Pupils have access to school e-mail accounts on the Trust system and must immediately tell a teacher if they receive offensive e-mail.

Website

The Trust's websites are designed to give information to the public, initially and primarily for parents, but is available to any interested parties. Staff or pupil personal contact information will not be published. The contact details given online relate directly to school offices. The content of the websites will guard against any reasonable risk to children through the published content, and nothing will be published which could lead to contacting a child. Photographs that include pupils will be selected carefully to ensure that only pupils where permission has been granted are used. Whenever possible, group photographs rather than full-face photos of individual children will be used and only with parental permission. Pupil's full names will not be used anywhere on a Trust website or other on-line space, particularly in association with photographs. Work can only be published with the permission of the pupil and parents/carers who are clearly informed of the Trust policy on image taking and publishing, both on Trust and

independent electronic repositories. The responsibility for this lies with all staff, who are responsible to the Headteacher and the CEO.

Social networking and personal publishing

The Trust controls access to social networking sites through the Trust filter, and refers to the nature of their use through PSHE sessions. Newsgroups are also blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers, especially for primary aged pupils, and pupils will be advised to use nicknames and avatars if ever using social networking sites.

Using Social Media for learning purposes.

Social networking sites should not be used/accessed by pupils in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate. Children's information or work should not be uploaded to such sites without prior parental permission.

Pupil's private use of Social Media

In terms of private use of social networking sites by a child, it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook and Instagram to name two.

Parents/carers private use of Social Media

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the website, email and verbal discussion.

School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion.

Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

In the case of inappropriate use of social networking by parents, the Headteacher will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy..

Guidelines for Parents/Carers:

- Parents **must not** post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the TSSMAT community.

Managing filtering

The Trust will work with the IT Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher who has a duty to report the materials through the appropriate channels. The Senior Leadership Team (SLT), including the ICT Lead, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing & webcam use

Video conferencing should use the educational broadband network to ensure quality of service and security. Pupils will only make or answer a video conference call in the presence of a teacher or member of staff at a pre-arranged time.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The senior leadership team is aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications, and as such mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. The use by pupils of cameras in mobile phones is not permitted in school.

The Trust does not currently have any games machines such as the Sony Playstation, Microsoft Xbox or others with Internet. If the use of these is permitted in future, they will be closely monitored due to the bypassing of Trust filters. Children will be educated that care is required when using these technologies

The appropriate use of Learning Platforms is discussed as the technology is used within the school.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

Guidelines for children

A printed copy of the **SMART** guidelines are kept next to the computer. The guidelines are explained to any children wishing to access the internet:

- **Safe:** Keep safe by not giving out personal information – such as name, email, phone number, address, or school name – to people who you don't trust online.
- **Meeting:** Never agree to meet anyone you have only met online unless your parent or carer is with you.
- **Accepting:** Do not accept emails or instant messages, or open files, images or texts from people you don't know. They can contain viruses or nasty messages.
- **Reliable:** Not all the information found on the Internet is reliable and people you meet online won't always be telling the truth.
- **Tell:** Tell a member of staff or your parents if someone or something you encounter online makes you feel uncomfortable.

Policy Decisions

Authorising Internet access

All staff must read and sign the Acceptable Use Policy before using any Trust ICT resource. The Trust will maintain a current record of all staff and pupils who are granted access to Trust ICT systems. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. Parents will be asked to sign and return a consent form for their child to access the Internet. Any person not directly employed by the Trust will be asked to sign the Acceptable Use Policy before being allowed to access the internet from a Trust site.

Assessing risks

The Trust will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Trust network. The Trust cannot accept liability for any material accessed, or any consequences of Internet access. The Trust will audit ICT use to

establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective annually.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a member of the SLT. Any complaint about staff misuse must be referred to the Headteacher or CEO. Complaints of a child protection nature must be dealt with in accordance with Trust Safeguarding procedures. Pupils and parents will be informed of the complaints procedure informed of consequences for pupils misusing the Internet. The Trust will liaise with local organisations and parents to establish a common approach to and understanding of e-safety.

Communication

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and Internet use will be monitored and appropriately followed up, and a programme of training in e-Safety will be developed, possibly based on the materials from CEOP. E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety policy

All staff will be given the Trust E-Safety Policy and its importance explained. Staff understand that network and Internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues. Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the Trust e-Safety Policy in newsletters, through parents' information evenings and on the Trust's websites. The Trust will maintain and publish a list of e-safety resources for parents/carers. The Trust will ask all new parents to sign the parent /pupil agreement when they register their child with the Trust. Schools send out an E-Safety Newsletter to parents/carers monthly.