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	September 2018
Next Review date	September 2019
Review Cycle	Annually
Statutory Policy	No
Publication	Website. SharePoint/Policies

E-Safety Policy

Summary

The E-Safety Policy is part of the School Development Plan 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 Securus software which flags up inappropriate content. The software reports incidences which are checked by the Richard Crosse School Secretary on a regular basis, and if required these are reported to the e-Safety Co-ordinator.

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 Local Authority when appropriate

Staff use a Trust phone when contact with pupils is required. 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
    - Securus is turned on
- The computers are located so that the screens can easily be seen from the rest of the room.
- Staff keep a close eye on 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 do not have access to 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 so that individual pupils cannot be identified or their image misused. 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. Please also refer to the Social Media Policy.

Managing filtering

The Trust will work with the Staffordshire LA 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 e-Safety Coordinator who has a duty to report the materials through the appropriate channels. The Senior Leadership Team (SLT), including the ICT coordinator, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

Videoconferencing should use the educational broadband network to ensure quality of service and security. Pupils will only make or answer a videoconference 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 are 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 SMT. 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.

Communications Policy

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.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Learning Zone The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kent Learning Zone Cluster Microsite blogs
Publishing pupils‟ work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils‟ full names and other personal information should be omitted. Pupils‟ work should only be published on „moderated sites‟ and by the school administrator.	Making the News SuperClubs Plus Headline History Kent Grid for Learning Cluster Microsites National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery

	Staff must ensure that published images do not breach copyright laws.	
Audio and video conferencing to gather information and share pupils‟ work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives “On-Line” Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Becta
http://schools.becta.org.uk/index.php?section=is
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kent e-Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/e-safety_home.cfm
Kidsmart
www.kidsmart.org.uk/
Kent Police – e-Safety
www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD
http://publications.teachernet.gov.uk
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Kent leaflet for parents: Children, ICT & e-Safety
www.kented.org.uk/ngfl/ict/safety.htm
Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com