St. Mark's C.E. Primary School

Redhouse Lane
Bredbury Stockport
SK6 1BX

www.st-marks.stockport.sch.uk

E-SAFETY POLICY

Author	**C. Stott**
Approved By (Committee / Group)	**Teaching and Learning**
Date Ratified by FGB	**Autumn Term 2017**
Where published / Displayed	**School Website / Staff Shared Area**
Review Date	**Autumn 2020**
Target Audience	**Staff, Governors & Parents**
Is this a Statutory Document?	**Yes**

Key Information:

This policy is a working document which reflects the current practice and procedures of E-Safety within St Marks and is updated regularly. It has been written with regard to the 'National Curriculum 2014' and is to be read alongside the Computing Policy. This policy applies to all members of the *school* community (including staff, students, pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of school IT systems.

Schedule for Development / Monitoring / Review

This online safety policy was approved by the *Board of Governing Body on:*	*Summer 2017*
The implementation of this e-safety policy will be monitored by:	*CS*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*E-Safety Policy will be reviewed and ıted annually in the light of new initiatives –*
Policies with reference and relevance to this policy:	*Safeguarding Policy* *Cyberbullying Policy* *Computing Policy* *Acceptable use policy*

Roles and Responsibilities

Governor with responsibility for Computing and IT:	
ESafety Subject Leader:	*CS*
ESafety Team	*CS – Focus on the teaching and learning of ESafety across the school.* *DA & DH – Focus on the Safeguarding within ESafety* *AW* *KQ* *Staff/TA/Admin Staff/Governors*

Key Information: IT Provision

The school is equipped with:	IPADs	70
	PC's	56
	Laptops	32
	Galaxy Tabs	2
	Interactive Plasma screen	6
	Whiteboard	11
	Macbooks	20
	Staff laptops	14
School Website:	*http://www.st-marks.stockport.sch.uk/*	

The importance of the internet:

Why do we need the internet?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.
Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.
Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient;
- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between students world-wide;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments; educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and The Department for Education.

How can Internet use enhance learning?

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use within a comprehensive, flexible and relevant computing curriculum that enables pupils to become safe and responsible users of new technologies.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including

the skills of knowledge location, retrieval and evaluation.

How do we promote E-Safety at St Mark's?

As part of its on-going commitment to support staff's professional development, the school conducts training for all staff. This training helps to progress their knowledge and expertise in the safe and appropriate use of new technologies. With technology changing rapidly school have recognised the importance to reflect upon the advances in technology and support staff in this area.

Staff Training

- Staff will regularly complete E-Safety training – this may be in the form of online training. There will be a saved record which informs the E-Safety Team as to who has completed the training. The training is compulsory for **all** staff at St Mark's.
- Reminders will be made to staff throughout the year of the procedures in place regarding E-Safety and will be made aware of any changes made as and when they it happens.
- Staff will be aware of all members of the E-Safety Team.
- Children will be taught E-Safety through the computing 'Key Skills'. The key skills are to be taught throughout the school year and assessments will be made by teaching staff termly/annually.

Pupils

- E-Safety will be promoted through circle times/school assemblies that will explore various aspects of the key topics within the E-Safety Key Skills (content, contact and conduct) throughout the school year.
- The 'Digital Leaders' will be used to promote E-Safety in school through different routes such as assemblies, displays, competitions, quizzes and activities.
- The school will celebrate 'Safer Internet Day' annually and will also promote E-Safety through 'Computing Day' during the summer term.

Parental Training

- A set of rules for Responsible Internet Use & E-Safety tips are on display throughout the school and on outdoor display boards for parents and children.
- Parents will be provided with reminders to promote E-Safety e.g. ESafety leaflets and Questionnaires
- As part of its on-going commitment to bridging the gap between IT systems at school and the more open systems outside school, the school conducts an audit of pupils' and families' views on E-safety with a view to ensuring children use new technologies safely and responsibly both at home and in school.

Authorised Internet Access

- Parents/carers will be informed that their child will be provided with their own supervised log in.
- Every child and staff member will have their own individual log in
- Internet access and parents/carers, as well as pupils and staff, will be asked to sign and return a consent form for Responsible Internet Use & E-Safety.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to Computing Subject Leader and the IT Technician (from MGL) and then recorded on a purple form, this will then be recorded in the E-Safety log by a member of the E-Safety Team. (Appendix A). The computer screen will be switched off/ screen turned around.
- School will ensure that the use of Internet-derived materials by pupils and staff complies with copyright law.

- Pupils are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher/teaching assistant if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Password Protection

- Names of staff/children will be written as initials and all documents sent via email will be password protected.
- The school issues passwords to all staff, including students and volunteers when appropriate.
- Staff and pupils are encouraged to change their passwords on a regular basis.
- Generic passwords are only used on a temporary basis for the purposes of demonstration or transition.
- Pupils must not disclose passwords to other pupils.

Social Networking

- The school blocks/filters access to social networking sites and newsgroups. Staff will have access to the schools twitter and facebook account through their 'Teacher IPAD' – Children will not have access to these devices.
- Parents will be reminded to 'request' access to the schools form of social media and will be blocked/'unfriended' if content is found unacceptable by the E-Safety Team.
- Pupils/Parents are reminded regularly of the age requipments for the indidivudal sites and these are displayed on the parent ESafety notice board.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.

Filtering

Internet access is controlled, maintained and filtered by our Internet Service Provider (ISP) which is Stockport MBC.

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the pupils' age.

USB memory sticks & other Portable Data Storage Devices

- Staff must not store sensitive data on unencrypted USB sticks/other data storage devices.
- Sensitive data must be stored on the school network or encrypted data storage devices.

Digital Cameras & iPads

- Staff must use school cameras and iPads to photograph pupils.
- In the event that a school camera is not available and with the Head teacher's permission, non-school cameras (i.e. the camera on a personal mobile phone) may be used to photograph pupils.
- If a personal device is used to photograph pupils, images/video be transferred to a school device or the school network and deleted from the personal device within 24 hours.

Storage of Photographs

- Photographs must be stored in a secure area within school network.
- Photographs must remain on school premises when practicable; for example, images taken during off-site school trips should be downloaded to the school network.
- Photographs must be deleted when no longer required.
- Current L.A. policy is adhered to regarding photographing & publishing images of children.

Mobile Phones & Other Hand Held/Communication devices

- Mobile Devices within school (eg school IPADs) must be locked in the classrooms secure cupboards and the key kept in a secure place when not in use.
- Mobile phones and other handheld communication devices are not to be used for personal use in the lesson or formal school time by pupils or staff.
- For the purpose of security, we recognise that parents/carers of KS2 children may want their child to bring a mobile phone to school. If this is required, at the beginning of the school day, all phones will be turned off and handed to the school office who will keep them in a safe place until the end of the day when they will be handed back to the child.
- Children are only allowed to turn on their mobile phone when outside the school grounds.
- Parents/carers will be asked to sign a consent form to authorise their child to bring a phone to school. Full responsibility for the phone will rest wholly with the parents/carers. KS1 children are not allowed to bring phones to school.
- Mobile Phone Bluetooth should be turned off.
- Sending of abusive or inappropriate messages is forbidden.
- Outside school hours, children are discouraged from taking mobile phone photographs and videos on the grounds of an infringement of personal privacy, image and child protection.

Managing Emerging Technologies

- Emerging technologies are examined for educational benefit and a (verbal) risk assessment will be carried out by the E-Safety Team before use in school is allowed.
- Mobile phones/handheld communications devices/gaming consoles are not used for personal use during lessons or school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Website

- The contact details on the website will be the school address, e-mail and telephone number. Staff members' or pupils' personal information will not be published.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of

pupils are published on the school website or social media. (Appendix A)

- **Photographs are not to be used if permission has not been granted by the parents. – All staff will be aware of pupils that are not to be photographed.**
- Photographs that include pupils will be selected carefully and will be appropriate for the context and, where possible, show the context.
- Pupils' full names will not be used anywhere on the website or social media in association with photographs.
- Pupils' full names will not be used anywhere to caption any photographs that are used in pupils' exercise books.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- The Sensitive Data Policy provides further information about the school's definition of sensitive data.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. That said the school recognises that by adopting a 'managed' IT system, pupils will develop a better knowledge of how to stay safe online as they develop the ability to assess and manage risk for themselves. Neither the school nor Stockport Council can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate every 12 months.

Handling E-Safety Complaints

- Any complaints of Internet misuse will be dealt with by a senior member of staff and recorded.

Safeguarding Officer or the Headteacher.

- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.