E-safety Policy

Date adopted	September 2011	**Owner**	Leri Brookbank
Last reviewed	September 2018	**Review cycle**	Annual

Introduction
This E-Safety Policy relates to other policies including those for Computing, Bullying and Safeguarding. The school E-Safety leader is Mrs Leri Brookbank. Our E-Safety Policy has been written by the school, building on best practice and government guidance. The E-Safety Policy and its implementation will be reviewed annually although any amendments will be made, if deemed appropriate, during the year.

Links to Learning

Why internet and digital communications are important
The Internet is an essential element in 21st century life for education, business and social interaction. The schools have a duty to provide students 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 school Internet access is provided by EAC Network Solutions and includes filtering appropriate to the age of pupils at this school. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content
The schools will seek to ensure that the use of Internet derived materials by staff and pupils comply 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. Pupils will be taught how to report unpleasant Internet content eg. using the CEOP Report Abuse icon of Hector Protector.

Managing Internet Access

Information system security
The schools' ICT systems and security software will be reviewed regularly. Virus protection will be closely monitored and updated regularly.

Emails
Pupils and staff may only use approved email accounts on the school system for any matters relating to school. Pupils must immediately tell a teacher if they receive offensive emails. Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission. Incoming emails should be treated as suspicious and attachments not opened unless the author is known. All pupil email communication will only take place within the online learning platform and any external communication will not be possible. All online activity will be closely monitored. The forwarding of chain letters is not permitted. Any emails to parents should either come from the school office account or be approved by a member of the ELT.

Published content and the school website
The contact details on the website should be the school address, email and telephone number. Staff or pupil's personal information will not be published. The ELT will take overall editorial responsibility and ensure that the content is accurate and appropriate.

Publishing pupil's images and work
Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name. The schools will seek to use group photographs rather than full-face photos of individual children. Pupil's full names will be avoided on the website or learning platform, as appropriate, including in blogs, forums, or wiki pages, particularly in association with photographs. Written permission from parents/carers will be obtained before photographs of pupils are published on the school website. Parents should be clearly informed of the school policy on image taking and publishing through the home contact book.

Social networking and personal publishing on the school learning platform
The schools will control access to social networking sites. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils must not place personal photos on any social network space provided in the school learning platform. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils will be advised to use nicknames and avatars when using social networking sites.

Defining 'sexting'
Whilst professionals refer to the issue as 'sexting' there is no clear definition of 'sexting'. Many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the internet'.

Creating and sharing sexual photos and videos of under-18s is illegal.

If a child within the school setting is involved with 'sexting' then the following procedures should be followed:

1. Do not view the imagery unless there is a clear reason to do so.
2. Refer immediately to a DSL within school with evidence.
3. DSL to discuss firstly with child, then parents/carers and if required to contact the police.
4. If the device needs to be seized and passed to the police then it should be confiscated, turned off and placed under lock and key by a DSL.

If children and parents follow our Mobile Phone Policy then this should not occur, as smart phones are not allowed in school. As per our policy, basic models, only under exceptional circumstances are allowed for children in Year 6 and should be retained in the school office during the day.

Managing filtering
The schools will work in partnership with EAC Network Solutions to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable online materials, the site must be reported to the E-Safety leader. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Mobile phones
General Use of Mobile Phones – Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. Mobile phones will not be used during lessons or formal school time except as part of an educational activity. It is strictly forbidden for both staff and visitors to use these devices to photograph children. Staff or visitors should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
Staff Use of Personal Devices – Mobile phones should be switched off and left in a safe place during lesson times. Staff should only use mobile phones in designated areas. The designated area is the staff room. Staff will use a school phone where contact with parents is required. If a private call needs to be made then a request for a room can be made to the ELT or the school office.

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. School cameras and tablet devices may be used within lesson time or for educational purposes only. The sending of abusive or inappropriate text messages is forbidden.

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

Wi-Fi
The school Wi-Fi is only available for approved school and staff devices.

Authorising Internet access
All staff must read and sign the 'Staff, Governor and Visitor Acceptable Use Policy' before using any school ICT resource. The schools will maintain a current record of all staff and pupils who are granted access to school ICT systems. Parents will be asked to sign a consent form.

Accessing risks
The schools will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The schools cannot accept liability for the material accessed, or any consequences of Internet access. The schools 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.

Handling E-Safety complaints
Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the E-Safety leader. Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet
All use of the school Internet connection by community and other organisations shall be in accordance with the school E-Safety Policy.

Introducing the E-Safety Policy to pupils
Appropriate elements of the E-Safety Policy shall be shared with pupils. E-Safety rules will be posted in all classrooms and all rooms with Internet access. Pupils will be informed that network and Internet use will be monitored. Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for pupils. Pupils will sign the E-Safety rules to say that they agree to follow the agreed rules.

Staff and the E-Safety Policy
All staff have access to the school E-Safety Policy and will have its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues. Staff will sign an Acceptable Use Policy to say that they agree to follow agreed rules.

Enlisting parents' support
Parents' and carers' attention will be drawn to the school E-Safety Policy in newsletters, the school brochure and on the school website. Parents and carers will, from time to time, be provided with additional information on E-Safety. The schools will ask all new parents to sign the parent/pupil agreement when they register their child with the schools.

Appendix One

E-Safety rules for KS2 Children
Be SMART

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we not sure about.
- We only email people an adult has approved or through the learning platform.
- We send emails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open emails sent by anyone we don't know.
- We do not use Internet chat rooms.

Class:

Date:

Signed by:

E-Safety rules for Infant and EYFS School Children
Be SMART

Think then Click

 These rules help us to stay safe on the Internet.

We only use the internet when an adult is with us.

 We can click on the buttons or links when we know what they can do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet. 

 We can send and open emails together.

We can write polite and friendly emails to people that we know.

Class:

Date:

Signed by:

Appendix Two

Staff, Governor and Visitor
Acceptable Use Agreement/ICT Code of Conduct

Introduction

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This Appendix supports our Staff Code of Conduct and should be read alongside this and is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

- I appreciate that ICT includes a wide range of systems.

We expect all staff to:

- Understand that it is an offence to use a school ICT system for a purpose not permitted by its owner.
- Only use the schools' email/Internet/Intranet/learning platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Executive Head Teacher or Governing Body.
- Comply with the ICT system security and do not disclose any passwords provided to me by the schools or other related authorities.
- Understand that I am responsible for all activity carried out under my username and will ensure that my computer is not left logged on when I am not in the classroom.
- To only use the approved, secure email system for any school business.
- To ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Executive Head Teacher or Governing Body.
- To not install any hardware of software without the permission of the schools' ICT technicians.
- To not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Know that images of pupils will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent/carer. Images will not be distributed outside the schools' network/learning platform without the permission of the parent/carer or Executive Head Teacher.
- Understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Executive Head Teacher.
- To respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the E-Safety leader, the DSL or Executive Head Teacher.
- Lock all computers (click the windows key and L) when not in use.

Appendix Three

ICT Parent/Carer Consent Form and E-Safety Rules

All pupils use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the E-Safety rules have been understood and agreed.

As the parent or legal guardian of the named pupil, I have read and understood the attached school E-Safety rules and grant permission for the child to have access to use the Internet, school email system, learning platform and other ICT facilities at school.

I know that my child has signed an E-Safety agreement form and that they have a copy of the school E-Safety rules. We have discussed this document and my child agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at St. Martin's C of E Voluntary Schools.

I accept that ultimately the schools cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the schools will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching E-Safety skills to pupils.

I understand that the schools can check my child's computer files and Internet sites they visit, and that if they have concerns about their E-Safety or e-behaviour that they will contact me.

I understand the schools are not liable for any damages arising from my child's use of the Internet facilities.

I will support the schools by promoting safe use of the Internet and digital technology at home and will inform the schools if I have any concerns over my child's E-Safety.

Parent/Carer name: ……..……..

Pupil name: ……..……

Parent/Guardian signature: ……

Date: ……..…..

Further information for parents/carers on E-Safety can be found at:
www.parentsprotect.co.uk and www.thinkuknow.co.uk

Please complete, sign and return to the school office.