Southwick CE Primary School

E-safety and Acceptable Use Policy

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of web filtering.
- Our e-Safety Policy has been written by the school, building on the Wiltshire e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

E-Safety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the e-safety basics are in place to support a range of activities.

Has the school an e-Safety Policy that complies with CFE guidance?	Yes
Date of latest update:	Feb 2020
The Policy was agreed by governors on:	
The Policy is available for staff	On the R drive
The Policy is available for parents	On request
The Designated Child Protection Coordinator is:	Lesley Shellard
The e-Safety Coordinator is:	Sarah Watkins
Has e-safety training been provided for both students and staff?	Yes
Do all staff sign an Staff Acceptable ICT Use Agreement on appointment?	Yes
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Yes
Have school e-safety rules been set for students?	Yes
Are these rules displayed in all rooms with computers?	By end T1 annually
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access (e.g. SWGfL).	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes

Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has 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.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include 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.
- 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 taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and 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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Sending images without consent, explicit images, messages that cause distress or harassment are not permitted.
- E-mails sent to an external organisation should be written carefully.
- The forwarding of chain letters is not permitted.
- Staff and governors must use secure e-mail for all professional communications via an official, school provided e-mail account.
- Phising emails – ensure you are mindful when opening emails that they are from a trustworthy source. (does it look and feel right?)
- If staff use their own device to access school emails then they should ensure their device is passwork protected (or thumb print) and they should use the Outlook app. Always ensure you sign out of application. Be mindful of any attachments opened/downloaded as these will be held on your device. Any data breaches could result in your personal emails be scrutinized by the ICO
- E-mails should only contain non-personal data; initials should only be used to identify individuals. Attachments with sensitive data should be password protected.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. She will be supported by the admin officer and the computer technician.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and wherever possible, will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

- The school will block/filter access to social networking sites e.g.Twitter, Instagram, Facebook etc.
- 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 will be taught about how to keep personal information safe and will be encouraged to set passwords, deny access to unknown individuals and make profiles private.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video-conferencing (see Remote Learning Policy)

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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.
- Mobile phones will not be used during lessons or formal school time. 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. Staff should use the password protected memory sticks provided to ensure safe transfer of pupil data

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Acceptable ICT Use Agreement' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
    - Parents will be asked to sign and return a consent form authorising internet use.

Use of mobile phones

Mobile phones should not be used by staff to make or receive personal calls during working hours. Phones should be placed in a handbag or cupboard and remain there except for the receipt of texts in case of emergency (at which point the HT or DHT should be informed). Urgent messages are best communicated via the office.

Mobile phones **must not** be used to take pictures of children or children's work. Staff should use school cameras/ipads only (which should remain on site at all times) for this purpose to ensure the safety of children. School ipads/camera will only be taken off site, by a teacher, when taking the children on a school trip.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor WC can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by the e-safety co-ordinator. 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.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety if the need arises.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- 'Think U Know' training materials will be used with pupils
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- 'Think U Know' training materials will be used with staff
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school web site

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 South West Grid for Learning
Using search engines to access information from a range of websites.	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 - Yahooligans - CBBC Search - Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail E-mail a children's author E-mail Museums and Galleries Links with other schools
Publishing pupils' work on school and other websites.	Parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News Infomapper Headline History SWGfL Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Where possible photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Facebook Making the News Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Not currently applicable