Swanmore Primary School

E-Safety Policy

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Curriculum, Child Protection and PSHE.

Our e-Safety Policy has been written by the school, building on County and Government guidance. It has been agreed by the staff, senior leadership team and approved by governors.

The e-Safety Policy will be reviewed annually.

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

- Responsible ICT use by all staff, governors and pupils; 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 content filtering.

Agreed by Staff:

Ratified by Governors:

Review Date: Summer 2014

Aims and Objectives of Internet Use

Why is Internet Use Important?

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 world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils 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 DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be 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.
- 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.

Acceptable ICT use

Authorised Access

- All staff, governors and pupils must follow the 'Acceptable ICT Use' sections of this policy.
- Parents will be asked to sign and return a 'Pupil Acceptable Use' form (see Appendix C) on behalf of their child/ren on admission to the school, usually by Year R teachers on initial home visits prior to beginning school. This form will remain valid until the child leaves Swanmore Primary.
- Staff and Governors will be asked to sign and return a 'Staff and Governors Acceptable Use' form (see Appendix D) on beginning employment at Swanmore Primary School.
- Any guest users can be allocated a guest login account and will be asked to sign an acceptable use form prior to using the machines.

World Wide Web

- If staff, governors or pupils discover unsuitable sites, the URL (address), time, content must be reported to the ICT subject leader or network manager who will contact the Local Authority helpdesk to block said site.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Particular Web-based tools that we use

Google Apps
As a school we will be trialling the use of Google Apps as a means of sharing learning between staff, children and parents. Each pupil in KS2 will have a unique 'Swanmore Apps' email address. They will also be taught how to select a strong password to protect this account.

Blogging
We use blogging to post information (text, photos, videos and audio clips) to a wider audience on the world wide web. Images and videos will be published in accordance with photo consent information received (see later). There is a link to the school blog on the school website homepage.

Social Media

As a school we recognise that social media and networking are playing an increasing role within everyday life and that many staff and governors are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff, governors and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks.

Staff and governors should:

- ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- not accept current or ex-pupils as 'friends' on social media sites such as Facebook. This is to ensure any possible misinterpretation. We do understand that some staff members live and have friends within the local community and ask that these members of staff take extra care when posting online.
- ensure that their communication maintains their professionalism at all times.
- be aware that electronic texts can be misconstrued so should endeavour to minimise the possibility of this happening.
- not use these media to discuss confidential information or to discuss specific children.
- check with the ICT subject leader or ICT technician if they need advice on monitoring their online persona and checking their security settings.

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that some are signed up with, or without, parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our ICT curriculum. We will ensure that parents are aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying occur.

School Trips

All parent helpers on day visits should be specifically asked not to take photos of other children. They should also be informed, as part of the briefing before leaving, that under no circumstances should images of children be shared on any social media site. Refer parents to Photo Consent form (signed on admission to SPS) if required.

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority

Filtering

The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.

We now operate FWF (Flexible Web Filtering) across the whole school. There is a small chance that certain key words with double meanings could result in age-inappropriate content being 'on screen'. The children will be taught about how to deal with this, should it occur, as part of the ICT curriculum.

Managing Emerging Technologies/ Future developments

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. This policy will be amended as required.

This academic year we will be trialling the use of touchscreen technology and which apps are suitable for educational use.

Use of Memory Sticks (and other portable storage)

All teaching staff have a memory stick for use as described in the 'Staff and Governor Acceptable Use Agreement'. In addition to this, staff will be told to minimize storage of sensitive and/or confidential information (e.g. reports, IEPs) on these devices.

Accessing the School Network at home

All staff will be able to access the school network from home when a home computer or a school laptop. It is vital that the 'Acceptable Use' agreement is strictly followed, as unauthorised changes (e.g. downloads, installations) could seriously affect the whole school network.

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, governors or pupils personal information will not be published.
- The network manager, headteacher and ICT subject leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Digital and Video Images

On entry to Swanmore Primary School parents/guardians will be asked to sign a photo consent form. For Year R children this would usually occur on home visits. For other children on admission to the school via the 'welcome pack'. The permissions will remain valid until one year after the child leaves or a change is requested by the parents/guardians. We will notify parents of this rule every September.

- If we do not have permission to use the image of a particular child, we will make sure they are unrecognisable to ensure they are not left out of situations unnecessarily.
- We will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.
- If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason. (See above.)
- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
- Photographs of swimming, changing for PE and other instances deemed inappropriate by class teacher will not be taken.
- Personal information about children or staff is not shared on our website. Contact e-mails are provided only for School office, Headteacher, and Website Administrator.
- All information on the school website is published by the website administrator, even if it is not written by him/her. This avoids content on the website inadvertently contravening these rules.

Assessing Risks

- The school 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. Neither the school nor Hampshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should review ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. This policy is reviewed annually, with termly health checks.

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 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

E-safety incidents will be responded to in accordance with the flowchart in Appendix A.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms (see Appendix B)
- Pupils will be informed that Internet use will be monitored.
- Sign ‘Acceptable Use’ agreement.

Staff and Governors

- All staff and governors will be given the School e-Safety Policy and its importance explained.
- Staff and governors should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Sign ‘Acceptable Use’ agreement.

Parents

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

Responding to e-safety incidents – Appendix A

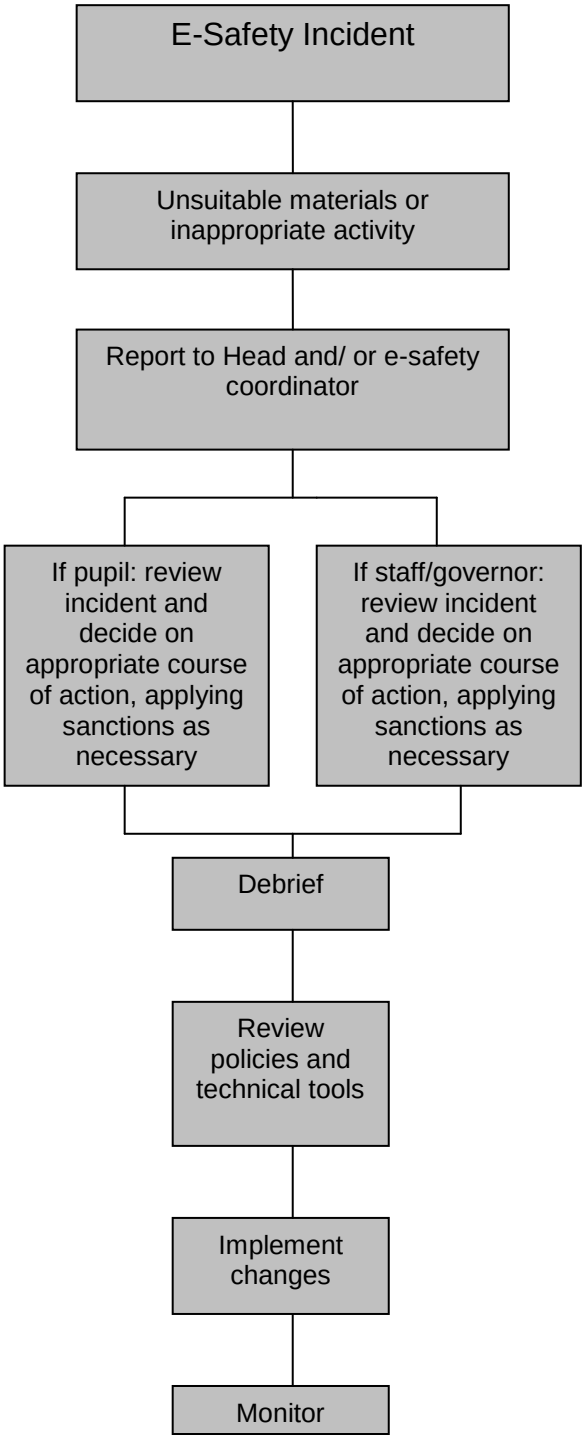
E-Safety Rules for KS1 and KS2 – Appendix B

Pupil Acceptable Use Policy – Appendix C

Staff and Governors Acceptable Use Policy – Appendix D

Appendix A

Flowchart for responding to e-safety incidents in Swanmore Primary School



Adapted from Becta – E-safety 2005

Appendix B

Key Stage 1

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 do.

- We can search the Internet with an adult.

- We always ask if we get lost on the Internet.

- We will share our passwords with our parents.

Key Stage 2

Think then Click

- We ask permission before using the Internet.
- We tell an adult if we see anything we are uncomfortable with.
- We only e-mail people an adult has approved.
- We send e-mails and messages that are polite and friendly.
- We never give out personal information or passwords but we can share them with our parents
- We never arrange to meet anyone we don't know.
- We do not open e-mails / messages sent by anyone we don't know.

Appendix C

Pupil Acceptable ICT use

E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as an email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Parental Signature:…… Date:……

Child's Name:…….. Class:……..

Appendix D

Staff and Governors Acceptable ICT Use
Staff Information Systems Code of Conduct

Purpose: To ensure that staff and governors are fully aware of their professional responsibilities when using information systems. Staff and governors should consult the school's e-safety policy for further information and clarification.

- I will use all software, hardware and data in a professional manner.
- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional rôle.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed:…… Date……