Swanmore Primary School

Online Safety Policy

Online 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 following are documents to be read in conjunction with the Online Safety policy:

- Social media policy
- Staff acceptable use policy + code of conduct
- Pupil acceptable use code of conduct

The Online Safety policy also operates in conjunction with the school's policies for Behaviour, Anti-Bullying, Curriculum, Child Protection, Safeguarding and PSHE.

Our Online 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 Online Safety Policy will be reviewed annually.

Online 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 (please see staff acceptable use policy/pupil code of conduct/social media policy)
- Sound implementation of Online 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.

Date of Policy Issue/Review:	July 2020
Reviewed and approved by Personnel Committee:	11th September 2020
Review date:	July 2021

1. 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.

2. Responsibility for online safety and acceptable ICT use

It is understood that everyone has a responsibility to ensure that they are using ICT responsibly and to help provide a safe environment for pupils, staff and governors when using ICT. When entering the school it is required that the following documents are read and signed:

- All staff and governors must follow the 'Staff acceptable use of ICT' policy and have signed the code of conduct. Staff and Governors will be asked to sign and return the code of conduct form on beginning employment at Swanmore Primary School.
- All pupils must have signed and follow the 'Pupil acceptable ICT use' code of conduct. 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.
- 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.

When using the Internet:

- 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.
- the 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.

Parents and Carers also play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents" evenings, newsletters, letters, website and information about national and local Online Safety campaigns/literature where appropriate.

3. 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.

4. 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

5. Filtering

The school will work in partnership with the Local Authority 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.

6. Managing Emerging Technologies/ Future developments

Emerging technologies will be examined for educational benefit. A risk assessment will be carried out for new technology that has potential risks before use in school is allowed. This policy will be amended as required.

7. The School's Online Use

Google Apps
As a school we make use of Google Apps as a means of sharing learning between staff, children and parents. Each pupil in KS2 has a unique 'Swanmore Apps' email address. They are taught how to select a strong password to protect this account and how to use email responsibly.
School website, Facebook and Twitter
These are used by the school to post information. For more information on the school's use of social media, please refer to the Social Media Policy.

8. 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.

- 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 full 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.
- Any photos of children should be taken using school cameras or tablets and uploaded onto the school network. Personal mobile telephones should not be used.

9. 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 Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate. This policy is reviewed annually.

10. Handling Online 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.

Online Safety incidents will be responded to in accordance with the flowchart in Appendix A.

Unacceptable ICT use by pupils:

The following table shows what actions will be taken in the event of a pupil misusing ICT within the school.

Pupil Incidents	Refer to class teacher	Refer to Headteacher	Refer to police	Refer to IT technician for action re filtering/security	Inform parents/carers	Removal of network/internet access rights	Further sanction e.g. detention/exclusion
Deliberately accessing or attempting to access material that could be considered illegal	☒	☒	☒				
Unauthorised use of non-educational sites during lessons	☒						
Unauthorised use of mobile phones/digital cameras/ other handheld devices	☒				☒		
Unauthorised use of social networking/instant messaging /personal email	☒			☒			
Unauthorised downloading or uploading of files	☒			☒			
Allowing others to access the school network by sharing usernames and passwords	☒	☒		☒		☒	
Attempting to access or accessing the school network using another student's/pupil's account	☒			☒		☒	
Attempting to access or accessing the school network using the account of a member of staff	☒	☒		☒		☒	
Corrupting or or destroying the data of other users	☒	☒		☒		☒	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☒	☒		☒		☒	☒
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☒	☒		☒	☒	☒	☒
Accidentally accessing offensive or pornographic material and failing to report the incident	☒			☒	☒		
Deliberately accessing or trying to access offensive or pornographic material	☒	☒		☒	☒	☒	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☒	☒		☒	☒	☒	

11. Communication of Policy

Pupils

- Pupils will be reminded by teachers to use the network and internet in an acceptable manner during online safety lessons.
- Pupils will be informed that Internet use will be monitored.
- Parents to sign 'Acceptable Use' agreement on behalf of their child.

Staff and Governors

- All staff and governors will be given the School Online 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 Online Safety Policy in newsletters, the school brochure and on the school Web site.
- Year R parents will be asked to sign the 'Acceptable Use' agreement on behalf of their child.

Appendices:

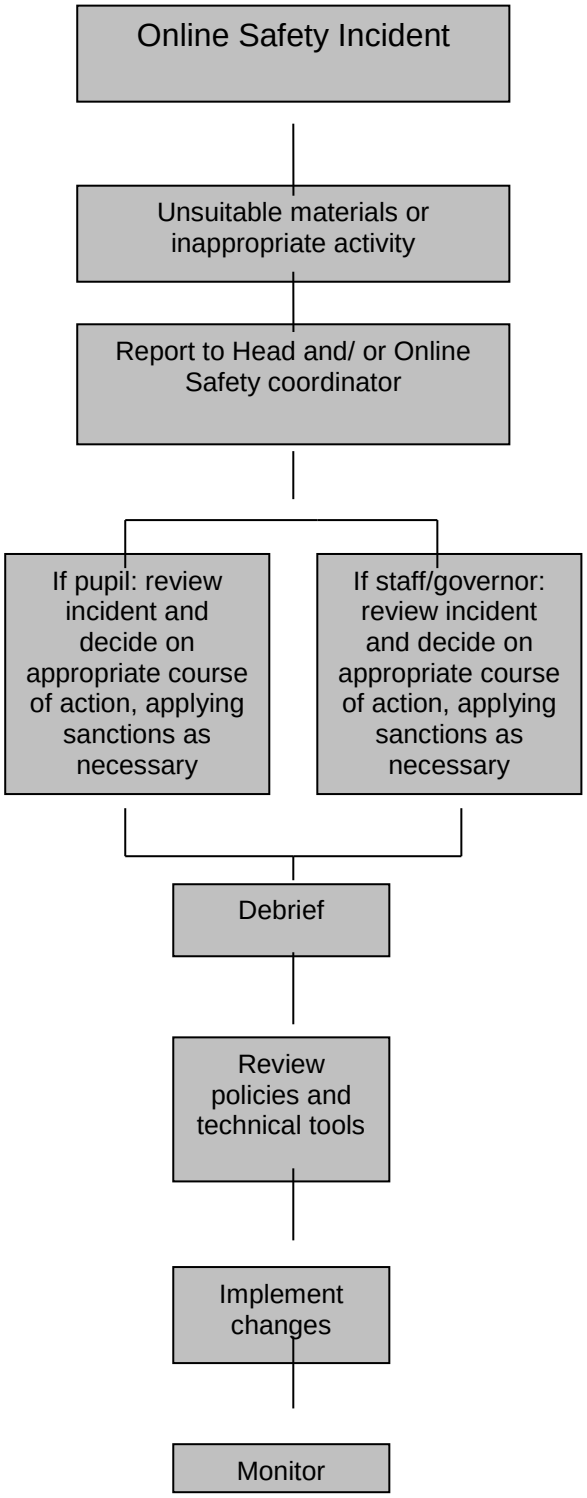
Responding to Online Safety incidents – Appendix A

Pupil Acceptable ICT Use – Appendix B

Staff and Governors Acceptable ICT Use - Staff Information Systems Code of Conduct – Appendix C

Appendix A

Flowchart for responding to Online Safety incidents in Swanmore Primary School



Adapted from Becta – E-safety 2005

Appendix B

Pupil Acceptable ICT use
Code of conduct

Online Safety Rules

These Online 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 school reserves the right to report or delete inappropriate materials where it believes unauthorised use of the school's computer system may be taking place.

Parental Signature:……. Date:……

Child's Name:…….. Class:……..

Appendix C

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 Online 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 be used for private purposes but must be done so following the school's Acceptable use policy.
- I understand that the school monitors 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 Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online 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 computer systems, including access to web-sites. The school reserves the right to report or delete inappropriate materials where it believes unauthorised use of the school's computer system may be taking place.

Signed:……. Date……

Print name: ……..