NOVEMBER 2024

E-Safety Policy

Swansfield Park Primary School

POLICY

Summary of Contents:

The purpose of this policy is to describe the safe use of the Internet and electronic communication technologies. It highlights the need to educate children and young people using new technologies both in and away from school. It also provides safeguards and rules to guide staff, pupils and visitors.

Any queries arising from this policy or its implementation can be taken up with the school's e-Learning Coordinator or the headteacher.

E-Safety Policy v1.4 SP Swansfield Park Primary School Version

Version Written by Andrew Johnson

E-Learning Coordinator, Swansfield Park Primary School

November 2024

(Adapted from Kent Schools Core e-Safety Policy, 2008)

1. Scope

1.1 This policy applies to all members of staff, trainees and other authorised users of the school's equipment and facilities, either on or off the school premises.

1.2 This policy should be read in conjunction with the school's ICT Code of Conduct and the school's IT & Information Security Policy. These are available on the school's network and School360 (Google Drive), or from the e-Learning Coordinator.

1.3 Additional related Policies include:

E-Mail Usage Policy - describing acceptable use of the council's e-mail system.

Internet Usage Policy - describing acceptable use of the council's Internet service.

Mobile Computing Policy - describing acceptable use of the school's mobile devices.

Use of Cameras and Mobile Phones Policy - describing safe & appropriate use of cameras and mobile phones.

Information Technology Security Policy - describing procedures to ensure the safe & secure use of the school's network & resources, & to protect systems & data from unauthorised access.

2. Introduction

2.1 The school has appointed an e-Learning Coordinator with responsibility for e-safety.

2.2 The Internet is an important element in modern life for education, business and social interaction.

2.3 The school has a duty to provide pupils with quality Internet access as part of their learning experience.

2.4 Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.5 This policy has three main objectives:

- To provide information on the safe use of the Internet and electronic communications technologies, such as mobile phones.
- To highlight the need to educate children about the benefits and risks of using technology both in and away from school.
- To provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

3. Responsibilities

3.1 The school's e-Learning Coordinator has responsibility for developing, reviewing and evaluating this policy.

3.2 The senior management team, school governors and the e-Learning Coordinator are responsible for the implementation and monitoring of this policy.

3.3 All users are required to formally acknowledge that they are aware of the E-Safety Policy and that they have read and understood its content.

3.4 All users of school IT equipment and facilities must ensure they adhere to the safeguards and rules provided in this policy.

3.5 All staff have a responsibility to educate pupils about the benefits and risks of using technology both in and away from school.

3.6 All staff must read and sign the Staff Code of Conduct for IT before using any school IT resource.

3.7 The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

3.8 In the Early Years and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

3.9 Parents will be asked to sign and return a consent form.

3.10 Any person not directly employed by the school will be asked to sign the Visitor Code of Conduct for IT before being allowed to access the Internet from the school site.

3.11 The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Northumberland County Council can accept liability for any material accessed, or any consequences of Internet access.

3.12 The school regularly audits IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

3.13 Complaints of Internet misuse will be dealt with by a member of the senior management team.

3.14 Any complaint about staff misuse of the Internet must be referred to the headteacher.

3.15 Complaints of a child protection nature must be dealt with in accordance with school child-protection procedures.

4. Teaching and Learning

4.1 The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.

4.2 Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for Internet use.

4.3 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4.4 Pupils will be taught how to evaluate Internet content and the importance of cross-checking information before accepting its accuracy.

4.5 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

4.6 Pupils will be taught how to report unpleasant Internet content or e-safety concerns, e.g. using the CEOP Report Abuse icon or the School360 Report a Concern button.

5. Managing Internet Access

5.1 Information system security

5.1.1 School IT systems security will be reviewed regularly.

5.1.2 Virus protection will be updated regularly.

5.1.3 Security strategies will be discussed with the IT support team.

5.2 E-Mail

5.2.1 Pupils may only use approved e-mail accounts within School 360.

5.2.2 Pupils must immediately tell a teacher if they receive offensive e-mail.

5.2.3 In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

5.2.4 Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

5.2.5 The forwarding of chain letters is not permitted.

5.3 Published content and the school web site

5.3.1 Staff or pupil personal contact information will not be published. The contact details given online should be staff work e-mails.

5.3.2 The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

5.4 Publishing pupils' images and work

5.4.1 Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. The school will use group photographs rather than full-face photos of individual children wherever possible.

5.4.2 Pupils' full names will not be used anywhere on a school website or other public on-line space, particularly in association with photographs. Full names may be used within the School 360 on-line space.

5.4.3 Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

5.4.4 Pupil image file names will not refer to the pupil by name.

5.4.5 Parents will be informed of the school policy on image taking and publishing.

5.5 Social networking and personal publishing

5.5.1 The school blocks access to social networking sites.

5.5.2 Newsgroups and forums are blocked unless a specific use is approved.

5.5.3 Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

5.5.4 Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

5.5.5 Pupils will be advised to use nicknames and avatars when using social networking sites.

5.6 Managing filtering

5.6.1 The school will work with Northumberland County Council to ensure systems to protect pupils are in place (Futures Cloud and Lightspeed).

5.6.2 If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Learning Coordinator.

5.6.3 Senior management, a designated governor, the e-Learning Coordinator and the school's IT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

5.7 Managing videoconferencing & webcam use

5.7.1 Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

5.8 Managing emerging technologies

5.8.1 Emerging technologies will be examined for educational benefit and an assessment carried out before use in school is allowed.

5.9 Mobile Phones

5.9.1 Technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to

undesirable material and communications; therefore, pupils are not allowed to bring mobile phones to school (see paragraphs 4.12, 4.13 and 4.14 of the Use of Cameras and Mobile Phones Policy for further details and exceptions).

5.9.2 Staff mobile phones must be switched off during lessons and should not be used in the presence of children (see Section 4 of the Use of Cameras and Mobile Phones Policy for further details).

5.9.3 Staff should have read and be familiar with the Use of Cameras and Mobile Phones Policy.

5.10 Protecting personal data

5.10.1 Personal data will be recorded, processed, transferred and made available according to the GDPR.

6. Communications Policy

6.1 Introducing the e-Safety Policy to pupils

6.1.1 E-Safety rules and advice (Smartie the Penguin, PenguinPig, SID's Top Tips, Think Then Click and/or S.M.A.R.T.) will be posted in all rooms where computers are used, displayed when children log on to school devices and discussed with pupils regularly.

6.1.2 Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

6.1.3 Children will be educated on e-safety issues using age-appropriate resources developed by Think U Know, Childnet, CEOP and SWGfL (e.g. Kara, Winston and the SMART Crew in KS2; Lee and Kim's Animal Magic Adventure in KS1; DigiDuck's Big Decision in EY; Smartie the Penguin and PenguinPig in EY and KS1; Project Evolve throughout school.)

6.2 Staff and the e-Safety Policy

6.2.1 All staff will be given access to the school e-Safety Policy and its importance explained.

6.2.2 Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

6.2.3 Staff that manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues.

6.2.4 Staff should always either use a child-friendly safe search engine when accessing the web with pupils, or should check search results prior to a lesson.

6.3 Enlisting parents' and carers' support

6.3.1 Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.

6.3.2 The school will maintain a list of links to e-safety resources and information for parents/carers on the school website.

6.3.3 The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

VERSION HISTORY			
VERSION	DATE	DESCRIPTION	AUTHOR
	June 2008	Core E-Safety Policy Template	Kent Schools
1.0 AS	Sept 2009	Alnwick South First School Version	Andrew Johnson
1.1 AS	Sept 2011	1.3, 5.5, 5.6	Andrew Johnson
1.2 AS	June 2013	5.5, 5.6, 4.6, 6.1	Andrew Johnson
1.0 SP	March 2015	Swansfield Park First School Version 1.2, 1.3, 3.6, 5.4, 5.9	Andrew Johnson
1.1 SP	Sept 2016	Swansfield Park Primary School Version 3.3, 3.10, 5.6.1, 5.9.1, 5.9.2, 6.1.1, 6.1.3	Andrew Johnson
1.2 SP	Sept 2017	5.10.1 Staff Use of Social Media Addendum	Andrew Johnson
1.3 SP	Sept 2021	1.2, 4.6, 5.10.1, 6.1.1, 6.3.2	Andrew Johnson
1.4 SP	Sept 2023	5.6.3, 6.1.3	Andrew Johnson
1.5 SP	Nov 2024	5.6.3	Andrew Johnson

APPROVAL AND AUTHORISATION				
	NAME	JOB TITLE	SIGNATURE	DATE
Adapted by	Andrew Johnson	E-Learning Co-Ordinator		November 2024
Approved by	Anne-Marie Grimes	Headteacher		November 2024
Approved by	Lauren Chapman	Governor		November 2024

DATE OF NEXT REVIEW	Autumn 2028

7. Staff Use of Social Media

Addendum September 2017

7.1 This addendum provides rules and guidance for staff to support their use of social media technologies.

7.2 Whilst the school does not advise staff against using social media for personal use, it does advise them to think carefully about the way they use social media technologies.

7.3 Professional Reputation

7.3.1 Staff need to be particularly aware of their online reputation, including what they choose to share and what information others post about them.

7.3.2 Staff also need to be aware of the reputation of the school and that they have a professional responsibility to ensure that their online actions do not negatively affect this.

7.3.3 Any staff member who shares content which may be libellous or bring the school into disrepute may be subject to disciplinary action.

7.3.4 Any staff member who criticises the school, employer, colleagues, pupils or parents online may be subject to disciplinary action.

7.3.5 Before posting or commenting on items, staff should consider whether they would be happy for their employer, colleagues, pupils and parents to see it. If not, then it shouldn't be posted in a public forum. This includes careful consideration of profile pictures.

7.3.6 Staff should be aware of being tagged in inappropriate pictures or posts which may affect their professional reputation or the reputation of the school. It is recommended that staff discuss their expectations around being tagged with friends and family, and ask them to be mindful of their professional reputation. In addition, many social media sites allow users to review tags before they are linked to their profile.

7.4 Contact with pupils and parents of pupils

7.4.1 Staff are not permitted to contact or befriend any current pupils or their siblings on social media. If pupils are consistently attempting to do so, report this to a member of the SLT.

7.4.2 Staff are strongly advised not to befriend former pupils, especially as they may have friends or connections to current pupils, unless the former pupil and their family have a 'real-life' social connection with the staff member outside of the school environment.

7.4.3 Staff are strongly advised to consider carefully the potential implications of befriending parents of pupils on social media. It is recommended that staff do not do so unless the parent has a 'real-life' social connection with the staff member outside of the school environment.

7.4.4 Staff should not share their personal phone number with pupils or parents. If it is necessary to contact parents, a school phone should be used.

7.5 Privacy

7.5.1 Social media sites have privacy settings and safety features to help you manage who can contact you and see the things you share online.

7.5.2 It is highly recommended that staff use the highest possible privacy settings. For advice on how to achieve this, staff can speak to the e-Safety Coordinator or visit *www.saferinternet.org.uk/safety-tools*.

7.6 Cyberbullying

7.6.1 Just like face-to-face bullying, cyberbullying of staff by parents or pupils will not be tolerated.

7.6.2 Staff are advised to regularly search their name in search engines and social media sites to check what information there is on the Internet about them.

7.6.3 If staff have offensive or hurtful information posted about them online, they should not retaliate to the message. Instead, they should make copies of all offensive content (including screenshots and URLs) and take them to the SLT.

7.6.4 The school will take action on cyberbullying in the same way as it would face-to-face bullying.

7.6.5 Staff can also report offensive material posted about them using the reporting procedures of the site involved, in order to get the material taken down.

7.7 Inappropriate content on social media involving pupils or parents

7.7.1 If staff see a young child on social media that is putting themselves at risk, or is involved in or the victim of inappropriate behaviour (such as cyberbullying or self-harming), they should report this to the SLT , e-Safety Coordinator and/or Designated Safeguarding Lead as soon as possible.

7.7.2 If staff see inappropriate comments about the school or other staff posted by pupils or parents online, they should make copies as evidence and inform the SLT.

This addendum was adapted from information provided by the NUT, ATL, Childnet and the UK Safer Internet Centre.

Staff who wish to seek further help or advice about keeping safe online can speak to the e-Safety Coordinator or the Professional Online Safety Helpline (POSH) - tel: 0344 381 4772 or e-mail: helpline@saferinternet.org.uk.

Further Information

Childnet - Teachers and Professionals Section
www.childnet.com/teachers-and-professionals

UK Safer Internet Centre - Teachers and School Staff Section
www.saferinternet.org.uk/advice-centre/teachers-and-school-staff

Social Media Guides
www.saferinternet.org.uk/safety-tools

Childnet - Teachers and Technology Checklist
www.childnet.com/ufiles/Teachers-and-technology-checklist.pdf

Professionals Online Safety Helpline (POSH)
0344 381 4772 or e-mail: helpline@saferinternet.org.uk

Childnet - How to make a report
www.childnet.com/resources/how-to-make-a-report

UKCCIS Sexting Guidance for Schools and Colleges
www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis