Swalwell Primary School

E-Safety Core Policy and Audit

Reviewed: November 2015

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets and wireless technologies 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 school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

The CFE Core e-Safety Policy

This core e-safety policy provides the essential basic. We consider that all the elements with a **red** bullet are mandatory in order to protect staff, pupils, the school and NCC.

End to End e-Safety

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

- Responsible ICT use by all staff and children; 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 from the Derwentside Network including the effective management of Website filtering.

- National Education Network standards and specifications.

E-Safety Audit

This quick self-audit will help the senior management team (SMT) 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 BECTA guidance?	Y
Date of latest update: November 2015	
The Policy was shared with governors on: December 2015	
The Policy is available for staff at: Staff Meeting, policy folder and on school website	
And for parents at: January 2015 (available on website)	
The Designated Child Protection Coordinator is: Mrs Lancastle-Smith and Mrs Waugh	
The e-Safety Coordinator is: Mrs Lancastle-Smith	
Has e-safety training been provided for both students and staff?	
Do all staff sign an ICT Code of Conduct on appointment? *This is updated yearly in September	Y
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules? *This is updated yearly in September	Y
Have school e-Safety Rules been set for children?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y

School E-Safety policy

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection.

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap- Mrs Lancastle-Smith to oversee in her capacity as Child Protection Officer and Mrs Waugh to liaise.

- Our e-Safety Policy has been written by the school, building on the Gateshead LEA and government guidance. It has been agreed by senior management and approved by governors .

- The e-Safety Policy and its implementation will be reviewed annually.

- The e-Safety Policy was revised by: Miss Waugh and Mrs Lancastle-Smith

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.

- 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 functions.

- Internet use is a part of the statutory curriculum and a necessary tool for learning.

- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

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. This will be given at the start of the academic year and continually referred back to, throughout the year by the teacher. The Esafety policy will be shared with children.

- 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.

- If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the LEA via the ICT subject leader/System Administrators.

- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

- The evaluation of on-line materials is a part of every subject.

- Pupils will use age-appropriate tools to research Internet content

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection and Forensic Software will be updated regularly.
- Security strategies will be discussed with Gateshead LEA.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

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 Head Teacher will take overall editorial responsibility and ensure that 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.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Parents or carers will be asked to notify school if they DO NOT wish for photographs or work of pupils to be published on the school Web site.

- Pupil's learning outcomes can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter 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 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 LEA, DfES 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

- 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.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

- Parents will be asked to sign and return the 'Acceptable Use Policy' at the start of each year in September.

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials such as the VLE.

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.

- 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 a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- 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.

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.
- Pupils will be informed that network and Internet use will be monitored.
- A record will be kept of any incidents of children accessing inappropriate websites.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and 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.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school web site www.swalwellprimary.org

LINKS TO OTHER POLICIES

Our E-Safety Policy links to the following school policies:

- Child Protection
- Race Equality
- Anti-bullying including Cyber Bullying
- Behaviour
- Tackling Extremism and Radicalisation Policy