Whalton with Longhorsley St Helen's
Church of England First Schools

Policy
for
e-Safety

Updated: Spring Term 2017
Approved: Spring Term 2017
Review date: Spring term 2018

What is E-Safety?

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, 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.

The school's e-Safety Policy will operate in conjunction with other policies including those for Good Behaviour, Anti – Bullying, Child Protection and Data Protection and Security.

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 from the Northumberland County Council Network including the effective management of Websense filtering.
- National Education Network standards and specifications.

Whalton with Longhorsley St Helen's C of E First School
E-Safety Policy

1. 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 ICT, anti-bullying and for child protection.

- The schools will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the schools, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors and the PTA.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by Mrs Brannen (Headteacher), and the e-safety co-ordinators (Mrs G. McEwan and Mrs P.Elliott)
- It was approved by the Governors in Spring 2017 and is reviewed and approved annually.

2. Teaching and learning

2.1 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.

2.2 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

2.3 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.

2.4 e-Safety in the Curriculum

- Children will have e-safety lessons as part of their ICT curriculum each term and all classrooms will have an e-safety display.

3. Managing Internet Access

3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be in line with Northumberland County Council. (Policy Central Enterprise)

3.2 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.

3.3 Published content and the school web site

- The contact details on the Website 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.

3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the Website or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Pupil's work can only be published with the permission of the pupil and parents.

3.5 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.

3.6 Managing filtering

- The school will work with the LA, 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.

3.7 Managing videoconferencing

- 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.

3.8 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.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 Policy Decisions

4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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.
- Parents will be asked to sign and return a consent form.

4.2 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 NCC 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.

4.3 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.

4.4 Community use of the Internet

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

5 Communications Policy

5.1 Introducing the e-Safety Policy to pupils

- e-Safety Rules will be posted in all classrooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

5.2 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.

5.3 Enlisting parents' support

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

Written and agreed by staff, this Policy was formulated after considering the following:

1. aims and content;
2. teaching strategies;
3. dissemination and consultation process.

Reviewed by staff, considered by Governing Body Curriculum Standards and Policies Sub Committee, approved at the Spring Term Governors Meeting and implemented from that date.

Appendix 1: E-Safety Audit – Whalton C of E First School

This quick audit will help the Senior Management Team (SMT) assess whether the basics of e-safety are in place. Schools will also design learning activities that are inherently safe and might include those detailed within Appendix 2.

The School has an e-Safety Policy that complies with CFE guidance.	✓
Date of latest update: **January 2017 (WHALTON)**	
The Policy was agreed by governors on: **30.1.17**	
The Policy is available for staff in the **School office**	
And for parents in the **School office and on the school website**	
The Designated Child Protection Coordinator is **Mrs Brannen**	
The e-Safety Coordinator is **Mrs P Elliott(Wh)**	
How is e-Safety training provided? **By NCC to Safety Coordinator then cascaded to staff**	
Is the Think U Know training being considered?	✓
All staff sign an Acceptable ICT Use Agreement on appointment.	✓
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	✓
Rules for Responsible Use have been set for students:	✓
These Rules are displayed in all rooms with computers.	✓
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access. (NorTLE)	✓
The school filtering policy has been approved by SMT.	✓
An ICT security audit has been initiated by SMT, possibly using external expertise.	✓
School personal data is collected, stored and used according to the principles of the Data Protection Act.	✓
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SMT.	✓

Appendix 1: E-Safety Audit – Longhorsley St Helen's C of E First School

This quick audit will help the Senior Management Team (SMT) assess whether the basics of e-safety are in place. Schools will also design learning activities that are inherently safe and might include those detailed within Appendix 2.

The School has an e-Safety Policy that complies with CFE guidance.	✓
Date of latest update: **January 2017 LONGHORSLEY**	
The Policy was agreed by governors on: **30.1.17**	
The Policy is available for staff in the **School office**	
And for parents in the **School office and on the school website**	
The Designated Child Protection Coordinator is **Mrs Brannen**	
The e-Safety Coordinator is **Mrs G McEwan**	
How is e-Safety training provided? **By NCC to Safety Coordinator then cascaded to staff**	
Is the Think U Know training being considered?	✓
All staff sign an Acceptable ICT Use Agreement on appointment.	✓
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	✓
Rules for Responsible Use have been set for students:	✓
These Rules are displayed in all rooms with computers.	✓
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access. (NorTLE)	✓
The school filtering policy has been approved by SMT.	✓
An ICT security audit has been initiated by SMT, possibly using external expertise.	✓
School personal data is collected, stored and used according to the principles of the Data Protection Act.	✓
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SMT.	✓

Appendix 2: 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 Northumberland 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 SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Focus on Film Northumberland Grid for Learning
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids 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.	SuperClubs Skype FlashMeeting
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.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum

Key Stage 1

Years 1 and 2 ICT Internet e-Safetv Rules

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 can send and open emails together	
	We can write polite and friendly emails to people that we know	

Key Stage 2

Years 3 and 4 ICT Internet e-Safetv Rules

Think then Click

e-Safety Rules for Key Stage 2

We ask permission before using the Internet

We only use websites that an adult has chosen

We tell an adult if we see anything we are uncomfortable with

We immediately close any webpage we not sure about

We only e-mail people an adult has approved

We send e-mails that are polite and friendly

We never give out personal information or passwords

We never arrange to meet anyone we don't know

We do not open e-mails sent by anyone we don't know

We do not use Internet chat rooms