



*The Ruskington
Chestnut Street CofE Primary School*

E SAFETY POLICY

Policy Co-ordinator: ICT Coordinator
Policy Dated : January 2013
Reviewed Policy Date: March 2016
Other Relevant Documents:

Presented to Governors: Next Full Governors Meeting
Date to be Reviewed: January 2017

1. Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

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

2.3 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

2.4 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.

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.

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 Web site 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 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.

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

- 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, DfE 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 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.
- The use of mobile phones as cameras is forbidden.

3.8 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. (see appendix 1)

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.

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.

5 Communications Policy

5.1 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.

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 newsletters, and on the school Web site.

Appendix 1 – Acceptable ICT Use Agreement

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to obtain permission from parents or carers before I can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people.
- I have read the procedures for incidents of misuse in the E-safety and Communication so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Senior Designated Person in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Senior Designated Person is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones to contact parents. Refer to communication policy for further details.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Headteacher prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have seen a copy of the E-safety and Communication Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed.....Date.....

Name (printed).....Chestnut Street CofE Primary School