ROTHWELL PRIMARY SCHOOL

E-Safety Policy Document

1. Introduction

1.1. The school makes widespread use of modern technology in the belief and understanding that it can develop and enhance all aspects of teaching and learning, as well as providing a preparation for life in a society where the use of ICT is widespread.

1.2. The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT.

1.3. This policy

- applies to all users of ICT equipment, in its widest sense, whilst on school premises. It also applies to anyone who uses school ICT equipment, software or electronic data whilst off the premises.
- forms part of the school's ICT subject policy and ICT acceptable use policy.
- relates to other school policies including, child protection, behaviour and bullying.
- also relates to the Leeds Learning Network Internet Access Policy & Email Code of Practice.
- often refers to the internet due to this being the major concern. However, it should be noted that there are other aspects of e-safety that need consideration.

1.4. It is difficult to consider every eventuality within this policy due to the nature of rapid technological change within short timescales.

1.5. **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, bullying and for child protection.

- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The appointed an e-Safety Coordinator is: …………………………..
- The e-Safety Policy was revised by: … … … … ……………………
- It was approved by the Governors on: … … ………………………….
- The next review date is (at least annually): … … ……………........

2.1 Teaching and learning

2.1.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.

2.1.2 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
- Pupils will be shown how to publish and present information to a wider audience (i.e. school website; podcasting; blogging)

2.1.3 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 will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

2.2 Managing Internet Access

2.2.1 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.

2.2.2 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.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

2.2.3 Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

2.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, 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.
- Work and Images can only be published with the permission of the pupil and parents/carers.

2.2.5 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- 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, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

2.2.6 Managing filtering

- The school will work with the Leeds Learning Network to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site 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.

2.2.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

2.2.8 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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones brought to school by children will be handed into a central location on arrival at school and collected at the end of the day.
- The use by pupils of cameras in mobile phones is not permitted within normal school hours.
- Staff will be issued with a school phone (Located in the Headteacher's Office; signed in and out) where contact with pupils is required or where mobile phones are used to capture photographs of pupils.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

2.2.9 Protecting personal data

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

Use of Ipads in Foundation stage

Staff in Foundation stage use the online profile system 2build a profile. Staff Ipads are kept separate to pupils Ipads and are protected with a pin.
The observations that form these profiles can be shared with parents via email called Parentshare.
Permission for sharing group photographs and observations will be gained at the start of each school year.
Observations will be emailed in a pdf format so that they cannot be altered or changed.

2.3 Policy Decisions

2.3.1 Authorising Internet access

- All staff must read and sign the school's 'Acceptable Use Policy' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Foundation stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- In Key Stage 2, children will also sign a consent form, agreeing abide by the 12 Rules for Responsible ICT Use.
- Any person not directly employed by the school (supply teachers; parents) who expected to access the school's curriculum network or use the internet will be asked to sign an 'Acceptable Use Policy – Staff' form before being allowed to access the internet from the school site.
- Supply staff will be provided with their own school laptop for their time in school once the Acceptable Use policy has been signed. The laptop will allow restricted access to the school network and, if access to LLN is needed, a designated Rainbow password will be used.

2.3.2 Assessing risks

- 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 KCC can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

2.4.3 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 (see schools complaints policy)*
- *Pupils and parents will be informed of consequences for pupils misusing the Internet. Not sure if as a school this needs including*

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, based on the materials from CEOP.
- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff should, where possible, use a child friendly safe search engine (e.g. cbbc; Yahooligans) when accessing the web with pupils.
- Staff should ensure that any searches that need to be completed by pupils are checked first.

2.5.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Acknowledgements

This policy has been adapted from Kent Schools Core E-Safety Policy 2008.