Ringway Primary School
E-Safety Policy

Date reviewed: March 2018
To be next reviewed: March 2019

Ringway Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?
- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones and I-Pads;
- Internet communications: e-mail and IM;
- Webcams and videoconferencing;
- Wireless games consoles

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. This e-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, whilst keeping safe and secure, and acting with respect for others. These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level.

Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

What are the risks?
- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft;
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

The flowchart attached as Appendix 1 illustrates our approach to investigating an incident of concern. This diagram should not be used in isolation when responding to incidents. As e-Safety is a relatively new concept and covers a wider scope than Internet use, a summary of a school's e-safety responsibilities is outlined below.

This list will assist in developing a co-ordinated and effective approach to managing e-safety issues:

- The school will appoint an ICT/E-Safety Coordinator.
- The ICT Coordinator will receive support and advice and training from an outside agency
- ICT E-Safety Officer, and where necessary, the police (CEOP's). The E-Safety coordinator should maintain the e-Safety Policy, manage e-Safety training and keep abreast of local and national e-safety awareness campaigns.
- The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.
- The school ICT E-safety officer will audit their filtering systems regularly to ensure that inappropriate websites are blocked.

- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.
- The school will include E-Safety in the ICT curriculum and ensure that every pupil has been educated about safe and responsible use.
- Pupils need to know how to control and minimise online risks and how to report a problem.
- All staff must read and sign the Acceptable Use Policy.
- Parents should sign and return the e-Safety rules contract each year for KS1, LKS2 and UKS2 children.
- The e-Safety Policy will be made available to all staff, governors, parents and visitors.

Implementation and Compliance

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences.

Teaching and learning

Why is Internet use important?

Developing effective practice in Internet use for teaching and learning is essential. 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. The Internet use is part of the statutory curriculum and a necessary tool for learning. 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. 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. 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:

- Internet access will be planned to enrich and extend learning activities.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils;

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity;
- Pupils will be educated in the effective use of the Internet in research, including the skills knowledge location, retrieval and evaluation.

Evaluating Internet Content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Local Area Network security

- Users must act reasonably;
- Users must take responsibility for their network use.
- For all staff, flouting electronic use policy is regarded as a matter for dismissal;
- Workstations should be secured against user mistakes and deliberate actions, e.g. deleting files and folders;
- Servers will be located securely and physical access restricted;
- The server operating system will be secured and kept up to date;
- Virus protection for the whole network will be installed and current;
- Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security

- All Internet connections must be arranged via Northumberland LA to ensure compliance with the security policy. Firewalls and switches are configured to prevent unauthorised access between schools.
- The security of the school information systems will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed with the LA when necessary;
- Personal data sent over the Internet should be encrypted or otherwise secured;

- Portable media may not be used without specific permission followed by a virus check;
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email;
- Files held on the school's network will be regularly checked;
- The ICT co-ordinator / network manager will review system capacity regularly.

Emails
- Pupils may only use approved e-mail accounts;
- 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;
- Whole-class or group e-mail addresses should be used in primary schools.

School Website and Learning Platform
The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. E-mail addresses should be published carefully, to avoid spam harvesting. The Head Teacher/ ICT Coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Use of Images.
Images that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social Networking
- The schools will block/filter access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations:
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers,

school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

- Pupils should be advised not to place personal photos on any social network space;
- They should consider how public the information is and consider using private areas;
- Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school;
- Teachers should be advised not to run social network spaces for student use on a personal basis.

Filtering

The school works with the LA to ensure that systems protect pupils and filter content by regularly reviewing and improving security. If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Coordinator. This task requires both educational and technical experience. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. School staff/ Visitors must not use mobile phones during lessons or formal school time. Pupils are not permitted mobile phones in school.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act1998.

Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications;
- All staff must read and sign the 'Staff Code of Conduct' before using any school ICT resource;
- At Key Stage 1 and 2, 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 for pupil access.

Internet Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Northumberland LA can accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

E Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff;
- All children will be taught to use the internet safely and the role of CEOP to monitor and report abuse;
- Any complaint about staff misuse must be referred to the Head Teacher, unless it is the Head Teacher where complaints will be sent to the Chair of Governors;
- Pupils and parents will be informed of the complaints procedure;
- Parents and pupils will need to work in partnership with staff to resolve issues.
- The e Safety rules are displayed in each classroom;
- Pupils will be informed that network and Internet use will be monitored;
- Safety training will be introduced to all to raise the awareness and importance of safe and responsible internet use;
- Instruction in responsible and safe use should precede Internet access;
- An e-safety module will be included in the PSHE, Citizenship and ICT programmes covering both school and home use;
- The e-Safety Policy will be distributed to all staff;
- Staff should be aware that Internet traffic can be monitored and traced to the individual user;
- Discretion and professional conduct is essential;

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues;
- Parents' attention will be drawn to the school's e-Safety Policy in newsletters and on the website;
- Internet issues will be handled sensitively, and parents will be advised accordingly.

Websites offering additional advice and guidance BBC Chat Guide:

http://www.bbc.co.uk/chatguide/ Becta
http://www.becta.org.uk/schools/esafety Childline
http://www.childline.org.uk/ Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk Grid Club and the Cyber Cafe
http://www.gridclub.com Internet Watch Foundation
http://www.iwf.org.uk/ Internet Safety Zone
http://www.internetsafetyzone.com/ Kidsmart
http://www.kidsmart.org.uk/ Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog Stop Text Bully
www.stoptextbully.com Think U Know website
http://www.thinkuknow.co.uk/ Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

This policy should be reviewed annually by ICT Coordinator and Senior Leadership Team.

Appendix 1

A concern is raised

Secure and preserve all evidence and hardware

If appropriate, seek advice and guidance from the Designated Officer for e-safety
(Russell Pilling)
01670 533622

Inform the Senior Manager / Headteacher and designated e-safety and/or child protection staff. Make a written record of the concern.

NCC & School Networks
Contact the Information Security Officer for assistance in establishing the type of activity - 01670 533309

Contact the Local Authority Designated Officer, LADO: Andrea Carmichael to discuss the need for further action - 01670 533503
To agree a strategy for dealing with the incident

Non-NCC Networks
Follow the relevant e-safety incident Reporting, and Child Protection procedures.

Agree a strategy for dealing with the incident

Are there any Child Protection concerns?

No

Yes

Refer to the relevant Information & Network Security Manager to consider further action

LADO will agree a strategy for intervention
Within 1 working day
Possible referral to:
- Northumbria Police Specialist Investigation Unit
- Children's Services
- FACT Locality Office

Standard child protection procedures will then apply.

Internal Action
This might include:
- Risk assessment
- Counselling
- Discipline
- Referral to other agencies
- Inform parents /carers if appropriate
Inform the Local Authority eg if a website needs blocking or child protection issues begin to emerge etc.

Report to the Designated Officer for E-safety
Within 7 working days

Consider whether the incident has procedural, training or security implications. Share the information appropriately