BIRLEY
Learning Community

Primary Phase

E-Safety Policy

September 2015 (Review September 2016)

E-Safety encompasses Internet technologies and electronic communications such as mobile phones 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. All education settings should be safe enviroments for children and young people to learn.

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 agreed local LA supplier

1.1 WRITING AND REVIEWING THE E-SAFETY POLICY

- Our E-Safety Policy has been written by the school, building on the LA and government guidance.
- The e-Safety Policy will be reviewed annually.

1.2 TEACHING AND LEARNING

1.2.1 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.

1.2.3 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 which Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide pupils in on-line activities that will educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the ICT Department.
- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

1.3 MANAGING INTERNET ACCESS

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the HGFL Broadband Service with its firewall and filters.

1.3.2 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 will 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.

1.3.3 Published content and the school web site/VLE

- 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 ICT Department will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupil’s images and work

- Pupils’ full names will not be used anywhere on the Web site, 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 is chosen carefully before publishing egg. If containing personal information

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.

1.3.6 Managing filtering

- The school will work in partnership with the LA chosen provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator or ICT Department.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing Videoconferencing

- Videoconferencing should only be carried out under strict supervision and follow the guidelines relating to electronic communications in general.

1.3.8 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.
- Pupils should not bring or use mobile phones at school or on school trips, unless previously arranged with the head teacher. The sending of abusive or inappropriate text messages is forbidden.

1.3.9 Protecting personal data

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

1.4 POLICY DECISIONS

1.4.1 Authorising Internet access

- All staff and pupils are granted Internet access, although access could be denied in the event of inappropriate use.
- At Key Stage 1 and 2, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

1.4.2 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, neither the school nor the LA can accept liability for the material accessed.
- The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/ Inclusion Team. Parents informed to consider steps to be taken.
- Any complaint about staff misuse must be referred to the head teacher/ DSL in school.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Lead or Deputy child protection officer.

1.4.4 Community use of the Internet

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

1.5 COMMUNICATIONS POLICY

1.5.1 Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

1.5.2 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.

1.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Reviewed by H Garratty / S Montgomery
February 2016