Berry Pomeroy
Parochial CE Primary School

E-Safety Policy

Rationale

Computers and the use of the Internet are a valuable resource for learners of all ages. It is increasingly providing the focal point of educational content in the 21st century. Schools acknowledge that computers and the internet do have the potential for inappropriate use and access to undesirable material and that we have a duty of care to protect our pupils. The purpose of this policy is to set out the procedures by which the school will minimise the misuse of computers and associated technology.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. The E-Safety Policy 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 E-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

The policy provides the essential minimum school e-safety standards. The purpose of these measures is to protect all users, the school and the LA.

Good Practice Regarding 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 Southwest Grid for Learning including the effective management of Web filtering.
- National Education Network standards and specifications.

Teaching and learning

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.

E-Safety policy
Agreed by FGB 25 April 2019
Review April 2020

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Possible teaching and learning activities include:
- Creating web directories to provide easy access to suitable websites.
- Using search engines to access information from a range of websites.
- Exchanging information with other pupils and asking questions of experts via e-mail.
- Publishing pupils' work on school and other websites.
- Publishing images including photographs of pupils.
- Communicating ideas within chat rooms or online forums
- Audio and video conferencing to gather information and share pupils' work.

Internet use will enhance learning
- The school Internet access is designed expressly for pupil use and includes appropriate filtering.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives/guidance for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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.
- Within the curriculum, children will be encouraged to consider the potential dangers of internet use in a variety of contexts

Managing Internet Access

Internet Access
- The school provides Internet access for educational purposes and should only be used by staff, pupils and members of the community for these purposes
- The school uses the Devon County Council recommended Internet Service
- Provider and connects to the Internet via the filtered service. Pupils cannot use computers without filtered access.
- Where reasonably possible, all Internet access by pupils is supervised by a member of staff or other responsible adult.
- Due regard will be given to children with Special Educational Needs to ensure that they have appropriate access to ICT
- No pupil, member of staff or community user is permitted to access material that is illegal or potentially offensive using school systems.
- The copyright and intellectual property rights of material accessed using the school system will be respected.
- Parents will be asked to sign a contract indicating that they give consent for their child to use the internet. This contract will also outline that pupils are expected not to

E-Safety policy
Agreed by FGB 25 April 2019
Review April 2020

actively attempt to access or distribute unacceptable material on school systems. This agreement to be reviewed and renewed annually.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with SWGfL & SCOMIS/DCC

E-mail - The use of e-mail is very limited in this school setting.

- 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.
- Children's e-mails should be written carefully and authorised by a member of staff or responsible adult before sending.
- The forwarding of chain letters is not permitted, and children are given advice how to deal with them outside school i.e. inform trusted adult and delete them.
- Any user of the school e-mail system must not use the system to communicate offensive, suggestive or defamatory material.
- E-mail messages sent and received from school systems should not be considered private. Pupils and staff should expect that e-mails could be inspected at any time.

Published content and the school web site

This school has its own web site. Ultimate responsibility for the content of the site rests with the headteacher and governors, in line with the following guidelines

- 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 without permission.
- The I.C.T. Co-ordinator/website administrator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not be identified by full name if labelled.
- Pupils' full names will not be used anywhere on the Web site
- 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 parental consent.

Social networking and personal publishing

- The school/ SWGfL will block/filter access to social networking sites.

E-Safety policy
Agreed by FGB 25 April 2019
Review April 2020

- Pupils will be advised never to give out personal details of any kind which may identify them or their location. This is part of our e-safety advice within school.

Managing filtering

- The school will work with the LA, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site by accident, it must be reported to the e-Safety Coordinator.
- Regular checks are made with the technician to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will be appropriately supervised for the pupils' age.

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

- Mobile phones will not be brought to school by children unless by prior arrangement with school. If a mobile phone is brought to school it will be kept securely in the front office. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Policy Decisions

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 have not been granted Internet access.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

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 authority can accept liability for the material accessed, or any consequences of Internet access.

E-Safety policy
Agreed by FGB 25 April 2019
Review April 2020

- The school will audit ICT provision yearly to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Any complaint about staff or pupil internet misuse must be referred to the headteacher.
  Complaints of a child protection nature must be dealt with in accordance with school child protection procedures

Communications Policy

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.

Staff and the e-Safety policy

- 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 computer. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy on the school Web site.

Useful websites

http://thinkuknow.co.uk/Default.aspx?AspxAutoDetectCookieSupport=1

http://www.childnet-int.org/kia/

E-Safety policy
Agreed by FGB 25 April 2019
Review April 2020