E-Safety Policy

Byker Primary School

Approved by:	Governing Body
Approved Date:	June 2023
Review frequency:	Annually
Next Review Date:	June 2024

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.

The previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for Positive Behaviour, Anti-Bullying with the Behaviour Policy, Curriculum, Data Protection and Security and Internet Use.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; 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 Newcastle LA Network including the effective management of Websense filtering.
- National Education Network standards and specifications.

School e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to the school's safeguarding policies and practices as well as to other policies including those for ICT, Anti-Bullying (as part of the Behaviour policy) and Child Protection.

- The school will appoint an e-Safety Coordinator. This will be the Designated Child Protection Coordinator as the roles overlap.
- 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 all staff and approved by Governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: Mrs Michelle Donnison Headteacher
- It was approved by the Governors: June 2023

2.2 Teaching and learning

2.2.1 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 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.
- 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.

2.2.2 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 as outlined in the Computing National Curriculum.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2.3 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- 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.

2.3 Managing Internet Access

2.3.1 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 Newcastle LA.
- 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.

2.3.2 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.

2.3.3 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless they have parental photographic permission.
- Pupil's work and photographs can only be published with the permission of the pupil and parents.

2.3.4 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 as part of the Computing National Curriculum. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail address, full names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

2.3.5 Managing filtering

- The school will work with the LA, DCFS 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.

2.3.6 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 are not allowed mobile phones in school, unless handed to staff for safe keeping.
- If necessary, staff will be issued with a school phone where contact with pupils is required.

2.3.7 Protecting personal data

☐ Personal data will be recorded, processed, transferred and made available according to current GDPR regulations – see privacy notices on school website.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read and sign the 'Internet Use Agreement' before using any school ICT resource.
- 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.
- Access to the Internet will be by monitored by adults with directly supervised access to specific, approved on-line materials.

2.4.2 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. Neither the school nor Newcastle LA can accept liability for the material accessed, or any consequences of Internet access.

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

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team and logged on CPOMS.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported to a Designated Safeguarding Lead.
- Pupils and parents will be informed of the complaints procedure.

2.4.4 Community use of the Internet

The school will liaise with local organisations to establish a common approach to esafety.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted on iPad trolleys and discussed with the pupils at the start of each term.
- E-safety will be referred to during lessons when using the internet
- Pupils will be informed that network and Internet use will be monitored.

2.5.2 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.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and the school brochure.
- Parent workshops will be held regularly to update parents on current issues related to e-Safety.