Ashley Primary School

E-Safety Policy

Date: May 2019

Review: Biannually

Staff Responsible:

Mrs. D Todd – Headteacher
Mrs. N Jewitt – Computing Leader
Mr. T Haram – Chair of Governors

Links to other Policies
The schools e-Safety Policy should operate in conjunction with other policies including those for Behaviour and Discipline, Anti-bullying, Safeguarding, Child Protection, School Acceptable ICT Usage Policy, CCTV Policy, Children's Acceptable Internet and Computer Usage Policy,

e-Safety Policy, Social Networking Policy, Computing Policy, Data Security Policy and Safe and Appropriate Use of Images Policy. This policy has been strongly influenced by the work of the South Tyneside LA E-Safety Team and the Open Zone@The Word.

Introduction
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.

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 including the effective management of filtering systems.

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 Computing and for child protection.

- The school's e-safety Leader is the also the Computing Leader. He/She works in close co-operation with the Headteacher and Deputy head.

- Our E-Safety Policy has been written by the school. It has been agreed by the staff and governors.

- The E-Safety Policy will be reviewed biannually.

Teaching and Learning
Why Internet use is important

- The Internet is an essential element in the 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.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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.

- Internet access will be planned to enrich and extend learning activities.

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them 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

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Coordinator.

- Staff should ensure that the use of Internet derived materials by staff and by 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.

Managing Internet Access
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 broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.

- 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 if not permitted.

Published content and the school website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

- The Headteacher 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 enable individual pupils to be clearly identified.

- 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 photographs of pupils are published on the school Website.

- Pupil's work can only be published with the permission of the pupil and parents.

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. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

Managing filtering

- The school will work in partnership with the service 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.

- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- IP videoconferencing should use the education broadband network to ensure quality of service and security rather than the Internet.

- External IP addresses should not be made available to other sites.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing should be supervised appropriately 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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- Staff have access to a school phone where contact with pupils is required.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.

- All Staff, including Teaching Assistants and Supply Teachers must read and sign the Acceptable ICT Usage Policy (AUP) before using any school ICT resource.

- At FS/KS1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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. The school can accept liability for the material accessed, or any consequences of internet access.

- The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

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.

- Sanctions with the school discipline policy include:
- interview/counselling by class teacher/Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period.

Reporting an e-Safety incident

- School follows the LA guidance and procedures.

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.

- Parents using school ICT equipment must sign an AUP consent form prior to use.

Communications Policy
Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.

- Pupils will be informed that Internet use will be monitored.

- Advice on e-Safety is built into the curriculum from year 1 – year 6 to raise the awareness and importance of safe and responsible internet use.

- Pupils will take part in Kidsafe sessions which directly relate to e-safety issues.

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.

- Staff will receive e-safety training.

Enlisting Parents and Carers support

- Parents and carers attention will be drawn to the School E-Safety Policy in newsletters and via the School website.

- Parental workshops run by staff/pupils will be held when deemed appropriate by the headteacher.

- Parental awareness of e-safety will be raised via class assemblies and participation in Safer Internet Days.