Holmleigh Primary School E-Safety Policy 2019

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Good Habits

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 London Grid for Learning (LGFL) including the effective management of content filtering using Atomwide.

The policy

Our e-Safety Policy has been reviewed by staff and approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed September 2020.

Why is Internet Use Important?

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 information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority; access to learning wherever and whenever convenient.

Teaching and learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils, while allowing staff to have access to some appropriate, but restricted sites using individual logins.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be 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.

An age appropriate scheme of work will be followed (digital-literacy.org.uk) by all classes from Year 1 to Year 6. This will comprise of an assessment to establish needs, 5 lessons, taught once every half term, followed by a reassessment to establish progress and areas that may need to be revisited in the second half of the summer term.

Nursery to use Smartie the Penguin to introduce the need to ask an adult – revisit several times throughout the year to remind pupils of the message.

Reception to use Hector's world lessons to introduce the online world.

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 The Learning Trust and with our ICT support provider.
- If taking equipment home, staff must ensure that all use is carried out in line with the schools e-safety, ICT and acceptable use policies.

E-mail

- Pupils may only use approved e-mail accounts on the school system, using pupil specific logins provided through LGFL.
- 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 by pupils 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.
- All staff will use school email system (Forename.Surname@holmleigh.hackney.sch.uk) for professional correspondence. These accounts can be monitored by the head, governors and the Local Authority.
- Access in school to external personal e-mail accounts may be blocked.

Published content and the school web site

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 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 Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published or used around school.

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.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- Staff will not associate with pupils on social networking sites.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

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, it must be reported to the Senior Leadership Team and ICT coordinator.
- Senior staff in partnership with The Learning Trust and LGFL will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 may use a school phone where contact with pupils or a parent is required.

Protecting personal data

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

Authorising Internet access

All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource.

Assessing risks

The school will take every possible precaution 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 LA can accept liability for the material accessed, or any consequences of Internet access.
The Senior Leadership Team/Subject Leader/e-safety group will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

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.
- Any complaints regarding e-safety will be recorded and will form part of a yearly review by the e-safety group to help to establish further training requirements and what adaptations to the e-safety curriculum and policy may be needed.

Community use of the Internet

The school will liaise with local organisations and the LA to establish a common approach to e-safety.

Communicating the Policy

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year in classrooms and in assemblies.
Pupils will be informed that network and Internet use will be monitored.

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 the individual user.
Discretion and professional conduct is essential.

Enlisting parents' support

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

Failure to Comply

Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by a senior member of staff.

Reviewed: September 2019
To be reviewed date: September 2020