Park Hill Primary School

E-Safety Policy

Definition

E-safety:

e-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- e-Safety concerns safeguarding children and young people in the digital world.
- e-Safety emphasises learning to understand and use new technologies in a positive way.
- e-Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- e-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

Effective Practice in e-Safety

e-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by all staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Use of a secure, filtered broadband (e.g. Broadband Sandwell);
- A school network that complies with the National Education Network standards and specifications.

E-Safety audit

Has the school an e-Safety Policy in conjunction with Sandwell Local Authority?		[✓ Y] / N
Date of latest update (at least annual):		September 2017
The school e-safety policy was agreed on:		January 2016
The policy is available for staff at:		School Website
The policy is available for parents/carers at:		School Website
The responsible member of the Senior Leadership Team is:		K.Cole
The responsible member of the Governing Body is:		M.Roberts
The Designated Child Protection Coordinator is:		C.Logan
The e-Safety lead in school is:		K.Cole
Has e-safety training been provided for pupils?	Ongoing	[✓ Y] / N
Has e-safety training been provided for staff?	04.09.17	[✓ Y] / N
Is there a clear procedure for a response to an incident of concern?		[✓ Y] / N
Have e-safety materials been obtained from recommended providers?		[✓ Y] / N
Do all staff sign a Code of Conduct for ICT on appointment?		[✓ Y] / N
Are all pupils aware of the School's e-Safety rules and acceptable use policy?		[✓ Y] / N
Are e-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?		[✓ Y] / N
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety rules and acceptable use policy?		[✓ Y] / N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?		[✓ Y] / N
Has an ICT security audit been initiated by the Senior Leadership Team, possibly using external expertise?		Y / [✓ N]
Is personal data collected, stored and used according to the principles of the Data Protection Act?		[✓ Y] / N
Is Internet access provided by an approved educational Internet service provider which complies with Department for Children, Schools and Families (DCSF) requirements (e.g. Broadband Sandwell)?		[✓ Y] / N
Has the school-level filtering been designed to reflect educational objectives and approved by the Senior Leadership Team? (Broadband Sandwell Filtering)		[✓ Y] / N
Is anti-virus up-to-date, and installed on all devices?		[✓ Y] / N
Are all shareholders aware of the CEOP Report Abuse button?		[✓ Y] / N

Teaching and Learning

Why the Internet and digital communications are 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 National 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.
- Pupils will be educated in the effective use of the Internet to research, including the skills of retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.

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 will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content by using the Child Exploitation and Online Protection Centre (CEOP) "Report Abuse" icon or "Hector Protector."
- Pupils will know to contact the named e-Safety lead in school if they experience any issues (K.Cole and SIPS IT Service)

Introducing the e-Safety policy to pupils:

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-Safety lessons will be taught in the Autumn Term, based on the materials from the Child Exploitation and Online Protection Centre (CEOP.)

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly by the ICT Technician/s. Virus protection will be updated regularly.

E-mail

Emailing within the school has been limited to staff only. All Staff have been assigned a Park Hill Primary School email address which is the main email used for all correspondences relating to the school. E-mails 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. Personal emails must not be used to send or receive school information, data or any information about children within the school.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Pupils' full names will not be used anywhere on the school Web site or other on-line space, particularly in association with photographs. Images of looked-after children will not be published. Written permission from parents or carers will be obtained before photographs/digital and video images of pupils are published on the school web site. Work can only be published with the permission of the pupil and parents/carers.

Managing emerging technologies

Mobile phones will not be accessible during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Staff will be issued with a school camera or an Ipad to capture photographs of pupils during school and Educational visits.

Authorising Internet access

All staff must read and sign the 'ICT Acceptable Use Policy' before using any school ICT resource.

Handling e-safety complaints

Any complaint about staff misuse must be referred to the Head Teacher. Complaints of a child protection nature will be dealt with in accordance with school child protection procedures. Staff can fill in an E-safety record of concern form and pass this on to the Head Teacher.

Staff and the e-Safety policy

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Staff will always use a child friendly safe search engine when accessing the web with pupils.

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

Managing filtering

If staff or pupils discover an unsuitable site, it must be reported to the Computing Leader/ICT Technician as soon as possible using the e-safety Incident log sheet. Frequent monitoring of internet usage will be conducted by SIPS IT/KC to ensure all users of school internet and IT facilities are within Policy guide-lines. Weekly reports will be generated and actions put into place if necessary.

Assessing risks:

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Sandwell Local Authority can accept liability for any material accessed or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Protecting personal data

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

School E-Safety policy Decisions

Policy Decisions

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the SLT/Headteacher
- Any complaint about staff misuse must be referred to the Head Teacher immediately
- Any complaint about Headteachers' misuse must be referred to the Chair of Governors immediately (M.Roberts)
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- An E-safety record of concern form must be completed by the member of staff and passed on accordingly to the Head Teacher.

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

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 ICT, bullying and for child protection.

- The school has appointed an e-Safety Coordinator/Computing leader; Mrs K Cole

- Our e-Safety Policy has been written by the school, building on the Sandwell e-Safety Policy and government guidance. It has been agreed by SLT and approved by governors.

Review:

The Policy will be reviewed September 2018.

Reviewed: September 2017

By: Mrs K Cole

Next Review: September 2017 or earlier if there are any changes to e-safety