Birch Hill Primary School

E-SAFETY & ACCEPTABLE USE POLICY

AUTUMN 2009

Contents

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, behaviour and for child protection.
- The school's E-Safety Coordinator is the Designated Child Protection Person as the roles overlap. It is not a technical role.
- Our E-Safety Policy has been written by the school. It has been agreed by all staff and approved by governors.

Teaching and learning

Internet Access

- 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.
- 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 in research, including the skills of knowledge location, 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

E-mail

- When available, pupils may only use approved e-mail accounts on the school system or "stickies" on the Fronter Learning Platform.
- Pupils must immediately tell a teacher if they receive offensive e-mail or "stickie".
- In e-mail or "stickie" communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mails and "stickies" from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Where possible group photographs will be used rather than full-face photos of individual children.
- Pupils' names will not be used in association with photographs anywhere on the school Web site or other on-line space.
- Pictures and work will only be shown on the website if parents/carers have signed the consent form issued at the start of each school year.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

- If they are to be used, the school will control access to social networking sites, and consider how to educate pupils in their safe use.
- 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, their friends or their location.
- Ideally pupils would use only moderated social networking sites, e.g. Grid Club.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing videoconferencing & webcam use

When available, videoconferencing and webcam use 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.
- Staff note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. These may not be used in school.

Protecting personal data

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

Procedures

☑ The School ICT system's security will be reviewed regularly.

☑ Virus protection will be updated regularly.

☑ Acceptable use posters will be displayed adjacent to all classroom workstations and on the two laptop trolleys.

☑ The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

☑ If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator and the school Network Manager and the E-Safety Coordinator informed.

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

☑ 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. The school cannot accept liability for any material accessed, or any consequences of Internet access.

☑ The school should 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.

☑ E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

☑ E-Safety briefings and materials will regularly be made available to parents.

☑ Staff will always use a suitable and safe search engine when accessing the web with pupils.

☑ Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

☑ Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.

☑ Staff must not use mobile phones during teaching time or use camera phones.

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 (see schools complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will ask all parents to sign the parent /pupil agreement at the start of each school year or when children are admitted in the case of in-year admissions.

Rules for Acceptable Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret;
- I will not access other people's files;
- I will only use the computers for school work and homework;
- Pupils should not download and use material or copy and paste content which is copyright. (*Most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should use information from the Internet.*)
- I will not bring in memory sticks or disks from outside school unless I have been given permission;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Display this page as a poster near computers and provide pupils and parents with a copy of these rules .