Lakeside Primary School: E-safety Policy

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, anti-bullying and for child protection.

➤ The e-safety coordinators are Jenny Rogers and Sam Fanzo.

➤ Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.

➤ The E-safety Policy and its implementation will be reviewed annually.

➤ The E-safety Policy was revised by: Sam Fanzo.

Teaching and learning

Why 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 curriculum and a necessary tool for staff and pupils

➤ Benefits of Internet use enhancing learning include deeper learning and research in a range of curriculum areas, communication skills and provides an opportunity for children to share work with a range of

➤ The school Internet access is provided by Surrey County through the RM contract and includes 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 appropriately to a wider audience.

Inclusion

➤ All children have equal access to Computing in order to develop their personal Computing capability. We ensure that Computing activities are fully inclusive for all children regardless of gender, disability, ethnicity, social class or educational need by:

➤ careful planning of groups to ensure that hands-on experience is equitable

➤ checking software, online resources and documentation to ensure that gender and ethnicity are reflected in a balanced way without stereotyping

➤ providing advice to teachers on the Computing support which can be offered to individual children with particular educational needs, including high ability pupils

➤ using external specialist support to assess a child's specific needs and providing specialist equipment or software

- ➢ being aware that some children do not have computers at home and ensuring that there are times when these children can have priority access to equipment
- ➢ taking every opportunity to provide children with access to technology at home through relevant grants and schemes
- ➢ ensuring good roles models amongst staff of Computing usage
- ➢ ensuring there is a balance in the activities provided to encourage collaborative work as well as competitive activities to suite different learning styles

Pupils will be taught how to evaluate Internet content

- ➢ The school will seek to 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
- ➢ Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access

Information system security

➢ School ICT systems security will be reviewed regularly
➢ Virus protection will be updated regularly
➢ Security strategies will be discussed with the Local Authority.

E-mail

➢ Pupils and staff may only use approved e-mail accounts on the school system – this includes a google classroom log in.
➢ 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.
➢ Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
➢ Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known .
➢ The school will consider how e-mail from pupils to external bodies is presented and controlled.
➢ The forwarding of chain letters is not permitted.
➢ Staff must not include full names and addresses of pupils in emails, and should use initials so they can't be easily identified. Care must be taken to ensure that emails do not contain inappropriate language or record personal information relating to behaviours, culture, or health that could cause offence if read by third parties.

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 head teacher or nominee 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. The school will look to seek to use group photographs rather than full-face photos of individual children
➢ Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs
➢ Permission from parents or carers will be obtained before photographs of pupils are published on the school Web site, blogs or used in marketing materials including brochure and advertisements.
➢ Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

➢ The school will advise about their access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords. School will not allow children to use social media (Facebook, Instagram, Twitter etc) within school and will remind children of the age limit and to be aware of weak passwords.

- The school will also remind children of the risks of posting photos, personal information and linking their account to the school.
- 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 must not place personal photos on any social network space provided in the school learning platform.
- 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 filtering

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site 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.

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.
- School iPads only to be used in school. Updates to be carried out regularly to ensure security on the devices.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with pupils and/or parents is required
- The appropriate use of Learning Platforms will be discussed when it becomes available to the children. Children will be encouraged to pick a secure password.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Teaching staff will be expected to use shared networks for work-related documents,. No personal data should be kept on home PCs or other removable devices.

Policy Decisions

Authorising Internet access

➤ All staff must read and sign the "'Acceptable User Agreement" before using any school ICT resource

➤ The school will maintain a current record of all staff and pupils who are granted access to school ICT systems

➤ At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials

➤ Parents will be asked to sign and return a consent form

➤ Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

➤ The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the 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.

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 head teacher

➤ 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.

➤ Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

➤ All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety policy to pupils

➤ Appropriate elements of the E-safety policy will be shared with pupils.

➤ E-safety rules will be posted in all networked rooms.

➤ Pupils will be informed that network and Internet use will be monitored.

➤ Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

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 that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' 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.

➢ Parents and carers will from time to time be provided with additional information on E-safety.

➢ The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.