Foresters 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 school's named e-safety coordinator is **Havard Spring.**

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

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 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. For example, this includes using the Internet for research, sending and receiving e-mail/messaging, coding through online resources such as Scratch and storing and retrieving information. The school internet access is provided by The London Grid for Learning through a regional broadband contract, which 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 safe, 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.
- 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 Childine.
- For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience acknowledging the lack of experience and internet at home.

- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

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.
- 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.

Published content and the school web site

- The contact details on the Web site should be the school address, email 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 pupils' 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

- 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 control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords. This control may not mean blocking every site it may mean monitoring and educating students in their 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 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 opportunities; however it does present dangers for primary and secondary 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 LFL|G 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.
- A log of any incidents may be useful to identify patterns and behaviours of the pupils.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing 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.

- 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.
- Handheld technologies, including games and mobile phones, often 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 is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

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

- All staff must read and sign the ‘Staff Code of Conduct for ICT’ 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 Sutton LA can accept liability for the material accessed, or any consequences of internet access.
- The school will monitor 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 and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

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.
- All staff will sign to acknowledge that they have read and understood the e-safety policy and agree to work within the agreed guidelines.
- 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.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents should be given e-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

- Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel interaction and exploration. Parents should be encouraged, where possible to interact with their children on the internet as well as provide other opportunities for learning and recreation

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

The e-safety Policy was revised by: Havard Spring

It was approved by the Governors on: 14/03/16