E-SAFETY POLICY
Roxeth Primary School
Revised February 2015

The E-Safety Policy is part of the school safeguarding agenda and relates to other policies including those for ICT, Bullying, Rights Respecting and for Child Protection.

The school has a designated E-Safety Officer who will work alongside the safeguarding leader to ensure safe usage throughout the school community.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. Our e-Safety Policy has been written, building on the Harrow e-Safety Policy and government guidance and will be reviewed every 3 years.

Teaching and Learning

Article 17 every child has the right to reliable information from the media

Why Internet use is important

- The Internet is essential in 21st century life for education. As educators we have a duty to provide pupils with quality Internet access as part of their learning experiences.
- Internet use is a part of the statutory curriculum and a necessary learning and teaching tool for staff and pupils.

Internet use will enhance learning

- The school internet access is subject to rigid filtering appropriate to the age of the pupils and some content and resources will be prohibited to safeguard staff and pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives.
- 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 will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing the School Network

- Ensure staff read and sign that they have understood the school's E-safety Policy. Following this, they are set-up with Internet, email and network access. Online access to services is through a unique, audited username and password.
- We provide pupils with an individual log-in username. From Year 1 pupils are also expected to use a personal password. All pupils use their own unique username and password which gives them access to the Internet and their own LGFL safe mail email account.
- We make clear that no one should log on as another user and make clear that pupils should never be allowed to log-on or use staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- We have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.

Managing Internet Access Information

- The school network and security will be reviewed regularly by the school's external IT support provider (Beebug) and our own IT Support based onsite.
- Virus protection is updated regularly.
- Security strategies will be discussed and dealt with by the in school's IT Support, Beebug and the Head Teacher.

E-mail

- Pupils may only use approved LGFL safe mail accounts when working on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail and this will be recorded on an E-safety incident log
- Pupils must not reveal personal details of themselves or others in e-mail or any online communications.
- E-mail sent to an external organisation should be written and constructed in a format appropriate for a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The Head Teacher is responsible for ensuring that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers: Marble Web Design and the schools IT support.
- The school web site complies with the statutory DfE guidelines for publications
- Photographs published on the web site will not have pupil names attached

Publishing images and work

Article 16 Every Child Has The Right To Privacy

- Photographs that include pupils, staff and governors will be selected carefully and will not enable individuals to be clearly identified unless relevant permission has been obtained
- Pupils' full names will not be used anywhere on the Web site and never in association with photographs.
- Written permission from parents/carers will be obtained when using pupil photographs.

Social networking and personal publishing

Staff

- No reference will be made in social media to students / pupils, parents / carers or school staff
- Do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions will not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Pupils

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be taught the reasons why personal photographs should not be posted on any social network space without considering how the photographs could be used now or in the future.
- Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- The school uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students.
- The school ensures the network stays healthy through use of Sophos anti-virus software etc. and network set-up so staff and pupils cannot download executable files.
- The school works with the LGFL and Beebug to ensure systems to protect pupils are regularly reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Officer and recorded on the E-Safety incident log
- Beebug and the onsite IT Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, students & parents' or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in the main office on arrival at school. Staff members may use their phones during school break times only.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited except where it has been explicitly agreed otherwise by the Head Teacher. Such authorised use is to be monitored and recorded.
- All mobile phone use is to be open to scrutiny and the Head Teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the school's telephone. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- The sending of abusive or inappropriate text messages is forbidden and should be reported, logged and followed up by the E-safety Officer and the Head Teacher.

Protecting personal data

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

Policy Decisions

Authorising Internet Access

- All staff, pupil's volunteers, parents / carers, visitors, community users must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who have been granted Internet access. This record will be updated regularly to ensure members of staff that have left the school's employment or pupil's who have left the school no longer have access to the school's network.
- Parents of KS1 pupils will be asked to read, sign and return a consent form giving permission for internet access

Assessing risks

- The school will constantly monitor all ICT access by both staff and pupils. Any inappropriate content will be reported directly to the Head Teacher.
- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints about staff misuse will be referred to the Head Teacher.
- Complaints about the Head Teacher must be reported to the Chair of Governors. Complaints or incidents will be recorded on an E-Safety incident log.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and referred directly to the Safeguarding Officer.
- Pupils and parents will be informed of the complaints procedure on the school website and a copy can be obtained from the school office on request.
- Close links and discussions will be held with the local community police to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Newly arrived pupils will access this information during induction sessions.
- Pupils will be informed that all network activity and online communications will be monitored
- Pupils will be actively encouraged to be vigilant when using devices and immediately report issues that may arise
- Pupils will be made aware and taught how to use the CEOP reporting button located on the school website

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will be made aware that Internet traffic will be monitored and will be traced to the individual user. Professional conduct is essential at all times.
- Staff should be aware that when unacceptable use is suspected additional monitoring and procedures may come into force.

Enlisting parents' support

Article 16 Every child has the right to Privacy

- A partnership approach with parents will be encouraged. This may include demonstrations, practical sessions and suggestions for safe Internet use at home. Parents will have access to sessions highlighting important e-Safety developments.
- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.
- Parents will be made aware and asked to reinforce the use of the CEOP reporting button located on the school website.
- The school operates an open door policy and encourages parents to talk to the E-safety officer if they have any concerns about their child and the use of E-safety. Roxeth takes Cyber bullying very seriously and will continue to educate the whole school community.
- During school performances some parents have requested for their child not to be photographed. Please respect their right by not filming and taking pictures during this time. Parents will be given the opportunity to take pictures at the end of every performance.