Barlby Primary School

E-Safety Policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying and for child protection. The school e-Safety Coordinator is Olivia Lacey.
Our e-Safety Policy has been written by the school, building on the RBKC e-Safety Policy 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.

Teaching and learning
Why Internet use is 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.

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. This will be taught in every module where the Internet will be used by the children.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Medium Term planning for units on Internet use will be available on the school network to ensure monitoring of objectives.

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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use child-friendly search engines and websites must be checked by school staff before introducing it to pupils.
- To avoid open ended internet searching, teachers will provide a folder of previously checked websites for children to use.

Managing Internet Access
Information system security

- The school maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with RBKC.
- Individual log-ins means activity on the network can be monitored and logged.

E-mail

- Pupils will be made aware of the risks and issues associated with communicating through e-mail and this is part of the school's e-Safety and anti-bullying education programme.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail. Any offensive emails will be printed and kept in an e-safety log, and the originals deleted.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- E-mail 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. A copy should also be sent to a member of SLT.
- 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, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. This permission can be withdrawn by parents or carers and consent must be given every two years.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site particularly in association with photographs.
- Text written by pupils should always be reviewed before publishing it on the school website.
- Class pages on the school Website are created by class teachers and are reviewed prior to posting. Images and pupils are carefully selected.

Social networking and personal publishing

- 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Staff will be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Managing filtering

- The school will work with the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator and ICT Coordinator so the site can be blocked.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- The school is registered with JVCS and all conferences are therefore timed, closed and safe.
- 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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff should be advised only to use their personal phone or camera for school business e.g. for a school field trip.

Protecting personal data

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

Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The ICT coordinator will keep a copy of these forms and they will be reviewed annually.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2 access to the internet will be supervised by adults and any websites the children are using will have been checked by the class teacher prior to the lesson.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor RBKC can accept liability for the 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 of Internet misuse will be dealt with by a member of SLT.
- 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety where appropriate.

Communications Policy

Introducing the e-safety policy to pupils

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

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.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Website.
- Workshops for parents will be organised to support them with e-safety
- The following websites are useful for parents who wish to know more about keeping their children safe online;
  www.thinkyouknow.co.uk - containing internet safety advice for those aged from 5 to 16, along with parents and teachers, this site is produced by CEOP (the Child Exploitation and Online Protection Centre).
  www.childnet.com/safety/ - helping to make the internet a great and safe place for children.
  http://www.vodafone.com/content/digital-parenting.html/# - this site is all about building children's confidence and resilience so that they get the very best out of the fast-moving, awe-inspiring, sometimes-overwhelming digital world.
  http://www.kidsmart.org.uk/ - learn about the internet and being a SMART surfer.
  http://www.childnet.com/resources/know-it-all-for-parents - lots of useful advice for keeping yourselves and your children safe on the Internet.https://www.discoveryeducation.co.uk/what-we-offer/discovery-education-espresso

Reviewed: Autumn 2018
Review Date: Summer 2019