Queensgate Foundation
Primary School

E. Safety Policy

September 2015

Working together for a successful future

E.SAFETY POLICY

Queensgate Foundation Primary School

Policy Review

This policy was adopted by the Governing Body on 17th October 2011 and will be reviewed in full by the Governing Body on a regular basis.

The policy was last reviewed and agreed by the Governing Body on 23rd September 2015

It is due for review on *Autumn 2019* (up to 48 months from the above date).

Signature ………………………… Head Teacher Date …………………

Signature ……………………….…Chair of Governors Date …………………

The e-Safety Policy is part of the ICT Policy and School Development Plan and relates to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship. Staff, parents, governors and pupils are involved in deciding the policy.

- The school's e-Safety Coordinator is Mr Peter Tilling.
- Our e-Safety Policy has been written by the school, building on the L.A. e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors
- The e-Safety Policy and its implementation will be reviewed annually.

1. Teaching and learning

Why Internet use is important.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- 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.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

The Government set a target that all schools should have broadband Internet use by 2006. Schools should have access to personal learning spaces by 2008 and learning platforms by 2010. A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.

The benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils world-wide
- vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with LA and DfES
- access to learning wherever and whenever convenient

How can Internet use 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 guidelines for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

- The schools will ensure that the copying and subsequent 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.

2. Managing Information Systems

How will information systems security be maintained?

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Governing Body and LA.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The ICT co-ordinator / network manager will review system capacity regularly.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive an 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.
- Whole-class or group e-mail addresses should be used in primary schools.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils’ personal information must not be published
- E-mail addresses should be published carefully, to avoid spam harvesting
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school’s guidelines for publications including respect for intellectual property rights and copyright

Can pupil’s images or work be published?

- Images 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 website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images of pupils are electronically published

How will social networking and personal publishing be managed?

- The schools will block/filter access to social networking sites
- 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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

How will filtering be managed?

- The school will work with the LA, Becta and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL 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
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later)
- The school’s filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by engineers

How will videoconferencing be managed?

The equipment and network

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer
- External IP addresses should not be made available to other sites
- Videoconferencing contact information should not be put on the school Website
- The equipment must be secure and if necessary locked away when not in use
- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled

Users

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing should be supervised appropriately for the pupils' age
- Parents and guardians should agree for their children to take part in videoconferences, probably in the annual return.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference
- Recorded material shall be stored securely
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class

How can emerging technologies be managed?

- 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
- The school should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy on phone use in school

How should personal data be protected?

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

3. Policy Decisions

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials
- Parents will be asked to sign and return a consent form for pupil access
- Parents will be informed that pupils will be provided with supervised Internet access

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use
- 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
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly

How will e-safety complaints be handled?

- 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

How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice

4. Communications Policy

How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access
- Pupils will be informed that network and Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use

How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and 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
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website
- Internet issues will be handled sensitively, and parents will be advised accordingly
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents
- Interested parents will be referred to organisations listed in section 3.0
  e-Safety Contacts and References

5. e-Safety Contacts and References

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta
http://www.becta.org.uk/schools/esafety

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

e-Safety in Schools
http://www.clusterweb.org.uk?esafety

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog

Stop Text Bully
www.stoptextbully.com

Think U Know website
http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/