



Online Safety Policy Of Queenborough School And Nursery



Headteacher: Mrs Barbara Conroy
Governor:
Name: Mrs Anna Glass
Date: January 2015
Review Date: January 2016

Queenborough School and Nursery

Online Safety Policy

Introduction

Our Online Safety Policy has been written by the school building on the Kent e-safety policy and Government guidance. The purpose of this policy is to ensure that all necessary steps are taken by the school to promote the care and welfare of its pupils with regards to online safety. The policy will be reviewed annually.

In today's society, children, young people and adults interact with technologies such as mobile phones, smart devices, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

The importance of Internet use

The use of Internet is part of everyday life for education, business and social interaction and we believe that we have a duty to provide pupils with high quality Internet access as part of their learning at Queenborough School and Nursery. Internet use is part of the statutory curriculum and a necessary tool for learning.

Pupils will be educated in the safe and effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet:

- Educational and cultural exchanges between pupils world-wide
- 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
- Access to learning wherever and whenever convenient
- Exchange of curriculum and administration data with KCC and DFE
- Access to world-wide educational resources including museums and art galleries

Enhancing learning

School Internet access will be designed to enhance and extend education. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

System Security

- Virus protection will be updated regularly.
- The security of the school information systems and users will be reviewed regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed in pupils' work areas.
- Files held on the school's network will be regularly checked.
- The LA ICT Technician and School Business Manager will review system capacity regularly.
- The use of user logins and password to access the school network will be enforced.

Email

Email is an essential means of communication for both staff and pupils. Directed email use can bring in significant educational benefits.

- Pupils will only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

Published content and the school website

The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information must not be published.

Pupil Images and work:

- Images that include pupils will be selected carefully and will not provide material that could be reused.
- 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.

Social networking, social media 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 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.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

Managing filtering

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with KCC and the Schools Broadband team to ensure that systems to protect pupils are reviewed and improved.
- The school will have a clear procedure for reporting breaches of filtering to SLT. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL must be reported to a member of the Senior Leadership Team who will then record the incident and escalate the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The school Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP.

Videoconferencing

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Including mobile communications, interact access, collaboration and multi-media tools. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Personal data

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

Authorising Internet Access

- 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 Acceptable Use Policy 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. At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- Parents will be asked to sign and return a consent form for pupil access (possibly as part of the Home-School agreement)

Risk Assessment

- 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 KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The Designated Safeguarding Lead will be informed of any Online Safety incidents concerns involving Child Protection concerns, which will then be escalated appropriately.

Handling complaints regarding Online Safety

- Complaints about Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

- All online safety complaints and incidents will be recorded by the school — including any actions taken.

Cyberbullying

- Cyber bullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007
- Cyber bullying (along with all forms of bullying) will not be tolerated at Queenborough School and Nursery.
- If an incident of cyber bullying occurs outside of school and the child's ability to work and feel safe are adversely effected, the school will work with parents and police to resolve the situation and possible sanctions can be put into place by the school (full details are set out in the school's policy on anti-bullying).

Learning Platforms -

- SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised on acceptable conduct and use when using the learning platform. Only members of the current pupil and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

Mobile Phones and Personal Devices:

- If a pupils brings a mobile phone into school then they must be handed in to the class teacher during the school day. Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

Communication of the Online Safety policy:

Pupils:

- An online safety training program will be introduced to raise the awareness and importance of safe and responsible internet use.
- All users will be informed that network and Internet use will be monitored.

- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Online Safety rules will be constantly reinforced and discussed with the pupils throughout each school year. Pupils will be reminded of the rules for keeping themselves online during lessons throughout the year.
- The Online Safety coordinator will regularly hold e-safety conferences with a range of children and vulnerable groups to monitor the children's awareness and understanding of e-safety. Findings will be relayed back to all staff and dealt with if necessary.
- The Think U Know website will be regularly visited by teachers throughout the year to support e-safety education. The website is also the school's homepage on the internet for staff and children to keep online safety awareness at the forefront of ICT education.

Staff:

- The Online Safety Policy will be formally provided to and discussed with all members of staff throughout the year to reflect the ever quick changing world of social media.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff iPads will not be allowed to have personal social networking apps, photo streaming from other personal devices, iMessage, magazines, books that could have inappropriate content for children.

Parents:

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website. Information and guidance for parents will be made available to parents in a variety of formats throughout the year.
- Parents will be requested to sign an online safety/Internet agreement as part of the Home School Agreement.

We confirm that this document is the school's official policy on online safety.

Headteacher: Mrs Barbara Conroy

Governor:

Name: Mrs Anna Glass

Date: January 2015

Review Date: January 2016