Queensmill School

E-Safety Policy

2019/20

C O N T E N T S

1. Introduction

Queensmill School recognizes that the Internet, and access to it via a range of technologies, is an attractive and increasingly integral feature of children's learning and entertainment. The school recognizes too that in enabling access to this invaluable resource it has a duty to ensure students are:

- safe from inappropriate content in a range of forms and across technologies
- safe from bullying and harassment of any kind
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared while online

It is the duty of the school to ensure that every child in their care is safe, and that safeguarding principles same should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks.

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many technological developments, there is also an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective e-safety Policy will help children to
develop the skills and confidence to manage potential risks and considerably reduce their impact.

Queensmill's e-safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our pupils are prepared to deal with the safety challenges that the use of technology brings.

The e-Safety Policy relates to other policies including those for safeguarding, ICT, bullying and for child protection.

The designated person for Child Protection is Mr Freddie Adu

The deputy Child protection Officer(s) Ms Joanna Dziopa and Mr Andy Nowak

2. Teaching and learning

2.1 Why the 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 pupils 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.

ICT will be used across the school to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences.

2.2 Internet use will enhance learning

The school's internet access will be designed expressly for pupil use. Access to the internet is enabled through the LGFL filter and where appropriate, the school will request changes to this filter.

Pupils will be taught what internet use is acceptable and what is not given and given clear information about what to do if they or anyone within school accesses unsuitable material or content which makes them uncomfortable.

Pupils will be educated in the effective use of the internet. This will have particular emphasis on what information they can and cannot share. There will be education too on the skills of knowledge location, retrieval and evaluation.

Pupils will be shown how to publish and present information to a wider audience.

2.3 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 the importance of cross-checking information before accepting its accuracy.

Pupils will be taught:

- What to do if they access inappropriate content (use of the 'safety' button and reporting to an adult)

- How to report unpleasant Internet content e.g. using the CEOP Report Abuse icon (www.ceop.police.uk

3. Managing Information Systems

3.1 Information system security

School ICT systems security will be reviewed regularly.

Virus protect will be updated regularly.

Security strategies will be discussed with the Local Authority.

3.2 E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

The forwarding of chain letters is not permitted.

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.

3.3 Published content and the school web site

The contact details given on the website will be the school address, e-mail and telephone number. Staff or pupil personal contact information will not be published.

The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupil's images and work

Written permission will be sought from parent/carers before photographs of pupils are published on the school web site.

Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Work can only be published with the permission of the pupil and

parents/carers. Pupil image file names will not refer to the pupil by name.

Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

3.5 Social networking and personal publishing

Social Network sites and newsgroups will be filtered unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for children and young people. Parents will be invited to the school to attend e-safety workshops aimed at raising their awareness of how to manage online content at home.

3.6 Managing filtering

The school will work with appropriate agencies and partners 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 school administrator or Head Teacher. This should be via the e-safety incident log which is monitored by the senior management

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing videoconferencing & webcam use

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

The use of webcams can only be used with the permission of the headteacher or other senior management.

3.8 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.

The senior leadership team have noted that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones are not permitted to be used in school useless agreed with the Head teacher. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The use by pupils of cameras in mobile phones will be kept under review.

Games machines including the Sony Play station, Microsoft Xbox and others potentially have Internet access. At school, these devices will only be available 'offline'. Staff will supervise pupils who access such devices.

The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

3.9 Protecting personal data

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

4 Policy Decisions

4.1 Authorising Internet Access

All staff must read and sign the Acceptable Use Policy for ICT before using any school ICT resource.

All pupils (or their parents if more appropriate) must read and sign the Acceptable Use Policy 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.

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.

4.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material, including providing appropriate close supervision. This will be achieved primarily by the LGFL internet filter. 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

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 and effective.

4.3 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 SMT

Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.

Pupils and parents are informed of the complaints procedure.

Pupils and parents will be informed of consequences for pupils misusing the Internet. This may include the loss of internet privileges.

5. Communications Policy

5.1 Introducing the e-safety policy to pupils

E-safety rules will be displayed around the schools and examples of good practice will be shared and promoted in assembly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in e-safety will be developed.

E-Safety training will be embedded within the ICT scheme of work and the PSHCE
curriculum.

5.2 Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

5.3 Enlisting parents' and carers' 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. Parents and carers will also have the opportunity to attend e-safety workshops hosted at the school to support and expand their knowledge of e-safety at home and outside school.

Where a pupil is unable to understand and sign the Acceptable Use Policy Parents will be asked to sign it so show they understand the expectations the school has of pupils in relation to e-safety.

The school will maintain a list of e-safety resources for parents/carers.

Policy reviewed – March 2019

Reviewed by ……F Adu……

Date for next review – March 2020