QEGS
BLACKBURN

E-SAFETY POLICY

This is a whole-school policy, within the framework of which the Primary School and the Nursery policies operate as appropriate.

This policy should be read in conjunction with the Acceptable Use Policies, Bring Your Own Device Policy, and Child Safeguarding Policy.

1. INTRODUCTION

1.1 The Internet is a valuable resource that can raise educational standards by offering pupils and staff opportunities to search for information from a very wide range of sources around the world. Some of the information to be found on the Internet, however, is inappropriate to Schools and the following policy helps to define appropriate and acceptable use by pupils/students and staff at the School.

1.2 The implementation of this policy is the responsibility of all members of staff.

1.3 The policy has been has been written with reference to the Think U Know (www.thinkuknow.co.uk) website and training literature.

1.4 Queen Elizabeth's Grammar School e-Safety Policy is available for parents on the School website..

2. ENSURING APPROPRIATE AND SAFE INTERNET ACCESS

2.1 The School has taken every practical measure to ensure that pupils/students and staff do not encounter upsetting, offensive or otherwise inappropriate material when they use the Internet in School. These include the following measures.

2.2 The School Internet Service Provider (ISP) is Schools Broadband and its service is filtered by 'Collaborative Filter' provided by Lightspeed Systems. This enables comprehensive management of web-browsing at a user level and includes detailed, customisable reporting.

2.3 To ensure that our systems are kept secure when using the web browsers neither pupils, students or staff are permitted to download plug-ins or extensions as this will compromise the security and the internet filtering system.

2.4 Pupil/Student E-mail

For pupils/students the School uses the off-site Google Apps for Educations service which gives users the familiar Gmail interface. Before any pupil/student E-Mail enters the School's systems it is filtered for spam / phishing by a cloudbased third-party service provided by Google. The content of these emails is also monitored for inappropriate language and phrases and if this is found, these emails are forwarded to the the Network Manager. Anti-virus and firewall protection technology (ESET) is resident on all PC computer systems in the School and ensures protection against E-

Mail-borne threats such as spam, viruses, and phishing. The E-Mail server also uses advanced E-Mail authentication techniques.

2.5 Staff E-mail

For staff, the School uses Microsoft Outlook and again this is monitored and filtered for spam and phishing through our Exchange Server. The School monitors staff internal and external e-mails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private.

When monitoring e-mails, the School will, except in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. However, where circumstances warrant it, the School may open e-mails and access the content.

2.6 Social Networking

Social Networking, Blogging and Newsgroups are blocked by the School's filtering systems. Some aspects of Twitter are allowed for use on the Twitter Feed on the School website. Facebook and other such sites are explicitly blocked. Youtube for Schools is allowed for pupils/students and the full Youtube site is accessible to staff only.

3. THE INTERNET IN SCHOOL

3.1 The School takes staff and pupils'/students' Internet safety extremely seriously and has devised a comprehensive plan for safe Internet use:

- Regular e-Safety awareness sessions will be embedded within the Computing scheme of work.
- Staff will check that the sites pre-selected for pupil/student use are appropriate to the age and maturity of the pupils.
- Staff will be particularly vigilant when pupils/students are undertaking their own searches and will check that the pupils/students are following the agreed search plan.
- Pupils/Students will be taught to use E-Mail and other Internet services responsibly in order to reduce the risk to themselves and others of exposure to inappropriate material.
- The School's Responsible Computer Use guidelines will be posted near computer systems.
- The Network Manager and Subject Leader of Computing will monitor the effectiveness of Internet access policies.
- The Network Manager and Subject Leaderof Computing will ensure that the e-Safety policy is implemented effectively.
- The Network Manager and Subject Leaderof Computing will ensure that all computer systems are routed through the School's Internet filtering systems.
- The School's methods to minimise the risk of pupils/students being exposed to inappropriate material will be reviewed frequently.

3.2 The School believes that the measures in place are highly effective. However, due to the linked nature of the Internet, it is not possible to guarantee that material of an inappropriate nature will not ever appear on computer screens at the School. The

School cannot, therefore, accept liability for the material accessed or any consequences thereof.

3.3 Pupils/Students at the School are taught to tell a teacher immediately if they come across any material that makes them feel uncomfortable. If there is an incident in which a pupil views offensive or upsetting material on a School computer the School will endeavour to respond to the situation quickly and on a number of levels as follows:

- Responsibility for incidents involving pupils will be taken by , the Network Manager and a Designated Senior Person for Child Protection.
- All the teaching staff will be made aware of the incident if appropriate.
- If staff or pupils/students discover unsuitable sites the Subject Leader of Computing and Network Manager will be informed.
- The website(s) in question will be added to a locally maintained list of banned URLs.
- It may be deemed appropriate to report specific websites to the Internet Watch Foundation (www.iwf.org.uk) and / or Child Exploitation and Online Protection Centre (www.ceop.gov.uk).

3.4 Pupils/Students are expected to play their part in reducing this risk by following the Acceptable Use Policy. These have been implemented to help protect pupils/students from exposure to Internet sites carrying offensive material. If unacceptable material is accessed deliberately by a pupil/student, then the teacher reserves the right to remove the privilege of using the Internet from that child until s/he proves that s/he can be more responsible. Further misuse will result in parents being informed after the Deputy Head has been notified and discussed the situation with the Head.

3.5 The School cannot accept any responsibility for access to the Internet outside School even if pupils/students are researching a topic related to School.

3.6 The Internet in School - Security of the School ICT Network

The Network Manager will ensure that the security strategies in place on the School's computer network are sufficient to protect the integrity of all networked computers. Access policies will be reviewed regularly and improved as and when necessary.

3.6.1 Because connection to the Internet significantly increases the risk that a computer of a computer network may by infected by viruses, or accessed by unauthorised personnel, the School's anti-virus protection and E-Mail protection are updated automatically and strict user polices are in place.

4. THE INTERNET IN THE CURRICULUM

4.1 Using the Internet to Enhance Learning

The Internet is an essential element in a 21st century School environment. Queen Elizabeth's Grammar School has a duty to provide pupils/students with reliable 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/students. Pupils/Students will be:

- Taught how to use a variety of web browsers.
- Taught what acceptable Internet use means and given clear guidelines for this.
- Educated in the effective use of the Internet for research, including the skills of retrieval and evaluation.

- Shown how to publish and present information to various audiences.
- Taught the importance of considering information before accepting its accuracy.

4.2 As in other areas of their work, staff recognise that pupils/students learn most effectively when they are given clear objectives for Internet use.

4.3 Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils/students:

- Access to the Internet may be by teacher demonstration.
- Pupils/Students may be given a suitable web page or a single website to access.
- Pupils/Students may be provided with lists of suitable websites which they may access.

4.4 Older pupils/students will be allowed to use the internet independently; pupils/students will be expected to follow the Acceptable Use Policy and will be informed that checks can and will be made on files held on the School's computer systems and the sites accessed.

4.5 . Pupils in KS2 will only be allowed to use the Internet once they have understood the Responsible Computer Use guidelines and accepted the need for these rules. It is unrealistic for pupils below KS2 to understand and accept these guidelines and so it is the teacher's responsibility to ensure they are kept safe while on-line.

4.6 Using Information from the Internet

In order to use information from the Internet effectively, it is important for pupils/students to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that most of the information on the Internet is intended for an adult audience, that much of it is not properly audited / edited and that a substantial percentage of it is copyrighted.

4.6.1 Pupils/Students will be taught to expect to find a wide range of content, wider than is found in the School library or on television.

4.6.2 Staff will ensure that their pupils/students are aware of the need to validate information whenever possible before accepting it as accurate, especially when considering non-moderated information from the Internet.

4.6.3 When copying information from the Internet, pupils/students and staff will be taught to comply with the laws of copyright, acknowledging authors and publishers when appropriate.

4.6.4 Pupils/Students will be made aware that the author of an E-Mail or web page may not be the person it appears to be.

4.7 Using E-Mail

Pupils will be taught how to use E-Mail applications and the conventions of using E-Mail to communicate with others. It is important that E-Mail communications are properly managed to ensure appropriate educational use, and that the good name of the School is maintained. To that end:

- Pupils will only be allowed to use E-Mail once they have been taught the Rules of Responsible Internet Use and understand these rules.

- Pupils/Students will be given individual addresses with the qegsblackburn.com domain name.
- The sending of E-Mails by pupils/students will be restricted to internal addresses only – those with an @qegsonline.com and qegsblackburn.com address.
- Pupils will be taught how to access their E-Mail accounts in School and under supervision of an adult at home.
- Pupils/Students may have the contents of E-Mail messages they compose checked by members of staff.

4.8 Social Networking and Personal Publishing

Queen Elizabeth's Grammar School prevents pupil/student access to social networking / blogging websites such as Facebook and Twitter using the School network. Pupils/Students are advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils/Students and parents are advised that the use of social network spaces outside School brings with it a range of dangers for pupils/students and that they should use extreme care when accessing social networking sites outside School. Social Networking, Blogging and Newsgroups are blocked by the School's filtering systems.

4.9 Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and the risks discussed before use is allowed in School. The Senior Management Team are aware that technologyies are continually changing and adapting and that this causes pressure on the wireless system. They are also aware that pupils/students using their own 3G/4G systems through mobile phones, ,smart watches etc could access inappropriate material if their own device is not fitted with age appropriate filters. All pupils and students are expected to follow the Acceptable Use Policy to minimise such breaches.
Pupils/Students at Queen Elizabeth's Grammar School are not permitted to use mobile phones or other communication devices during lesson time unless instructed to do so for a learning purpose. Any unauthorised device which connects to the School's Wi-Fi will be automatically redirected to a logon prompt, blocking access to the Internet until this user has gained permission and credentials to access the Internet from this device. All wireless devices connected to the School's Wi-Fi are monitored.

5. THE SCHOOL WEBSITE

5.1 Publishing Pupils'/Students' Images and Work

Currently parents are advised that if they do not wish the School to publish images of their child on the School website or in other promotional material then they should write to the School. Unless a parent/guardian advises the School of their wish they will not then be informed individually before the publishing of photographs/videos and/or samples of pupil's/student's work on the School website

5.2 Queen Elizabeth's Grammar School Website (www.qegsblackburn.com) is intended to:

- Provide accurate, up-to-date information about the School.
- Promote the School.
- Celebrate pupils'/students' work and achievements.

5.3 The Director of Marketing and Admissions and the Assistant of Admissions and Marketing are responsible for uploading content to the School website, and for ensuring that the links work and are up-to-date, and that the site meets the requirements of the site host.

5.4 The website is DDA compliant and exceeds the global WCAG 2.0 Level 2 standard and many of the Level 3 requirements (this being the most stringent accessibility standard). By reaching this standard the site will also comply with all other international standards. Current parents will also be able to access information specific to them via a password protected page. The password will be changed regularly to ensure a degree of security.

6. MONITORING

6.1 All teachers are responsible for monitoring the use of the Internet within their classrooms and for ensuring that unacceptable material is not accessed. This can be ensured in the majority of ICT suites using the Impero software which allows specific sites to be allowed or blocked and for whole class and individual pupil monitoring and access management.

6.2 The Subject Leader of Computing and Network Manager have responsibility for checking that no inappropriate material is on the School system, and the children are made aware that teachers have access to all their folders of work and can monitor their use of the internet and School IT systems. The Network Manager also ensures that the computer system is regularly checked for computer viruses.

7. POLICY REVIEW

7.2 This e-Safety Policy will be presented to the Governors for approval annually.

Updated by Mrs CY Gammon: August 2017

Approved by Board of Governors: June 2016