ACCEPTABLE USE POLICY - PUPILS

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

The use of the latest technology is actively encouraged at Queen Elizabeth's Grammar School. With this comes a responsibility to protect pupils and the school from abuse of the system.

The use of ICT must be in support of education and research in accordance with the educational goals and objectives of Queen Elizabeth's Grammar School.

Use of other networks or computing resources must comply with the rules appropriate to that network. (e.g. within visits to other schools or when on work placement)

Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws.

All pupils must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices (such as mobile phones, smart watches, iPod touches and iPads) within the school, irrespective of who owns the device.

Pupils are expected to behave responsibly on the school computer network and with the ICT equipment, as they would in classrooms and in other areas of the school.

Queen Elizabeth's Grammar School recognise the rapidly changing nature of the area of technology and affirms that, in all cases - even ones not specifically mentioned - the spirit and intention of this policy is to be followed.

Personal Responsibility

As a representative of the Queen Elizabeth's Grammar School, I will accept personal responsibility for reporting any misuse of the network to a staff member. Email, messaging, SMS or other forms of online communication must not contain anonymous, insulting, indecent, bullying, racist, sexist or homophobic messages, images or data.

1) Access

As a pupil at Queen Elizabeth's Grammar School, I have access to the following ICT facilities:

1.1 Specific computer devices throughout the school site. Pupils are not allowed to access computer devices reserved for staff including the teacher's computer in classrooms.

1.2 A secure username and password for logging into school computer systems

1.3 An accredited, filtered Internet connection from any computer in school or wi-fi connected device

1.4 Personal user space on the school network

1.5 Personal Google Drive with unlimited storage

1.6 A personal @qegsonline.org email account, via Google Apps for Education, with unlimited storage.

1.7 Access to network printers.

1.8 Access to resources such as desktop PCs, micro-computers, mobile devices and peripherals.

1.9 Access to online resources:
i. Google Apps for Education including Google Docs, Slides and Sheets
ii. Google Classroom as a VLE and class forum

1.10 I will only bring my home laptop or tablet (such as an iPad) into school having obtained the school's full permission beforehand (and having had a consent form completed and signed by a parent or carer). See Bring Your Own Device Policy.

2) E-safety

2.1 I will ensure that I am aware of e-safety issues affecting young people. I will visit www.ThinkuKnow.co.uk and ensure that I have read the guidance provided.

2.2 I will only email people I know or that my teacher has approved

2.3 The messages I send, or information I upload, will always be polite and sensible

2.4 When I use internet sites, I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends unless my teacher has given permission

2.5 I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room unless my parent or guardian has given me permission and I take a responsible adult with me

2.6 If I see anything I am unhappy with or I receive a message I do not like I will not respond to it but I will tell a member of staff.

2.7 If I access inappropriate material by accident (e.g. on a website) I will tell a member of staff.

2.8 I will always be myself and will not pretend to be anyone or anything that I am not on the internet

2.9 I will not use email or any communication technology to bully or harass others and I will report instances of online bullying to a member of staff

2.10 I understand that if someone makes me an offer via email or the internet that seems too good to be true, it probably is.

2.11 If I am in doubt I will ask a teacher or another member of staff.

2.12 Electronic mail (email) is provided by the School, the use of Internet based email systems is forbidden. Email, messaging, SMS or other forms of online communication must not contain anonymous, insulting, indecent, bullying, racist, sexist or homophobic messages, images or data.

2.13 I will not send large volume emails (spamming).

2.14 I will not use the School Internet for ordering goods or services regardless of their nature. I understand that it is also forbidden to subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature.

3) Computer security

3.1 I will keep my password secure (secret) and will not give it to anybody else to use

3.2 I will log off whenever I finish using a school computer

3.3 If I think someone else has my logon details I will report it to a member of staff

3.4 I will use computers with care and leave ICT equipment as I found it. I will not tamper with computer systems or devices (e.g. printers and projectors) and their cabling

3.5 I will tell a teacher if I notice that ICT equipment or software is damaged or not working correctly

3.6 I will not try to bypass security features or systems in place on the network or try to access anyone else's user account (hacking).

3.7 If I find that I do have access to an area that I know I should not have access to, I will inform a member of staff immediately.

3.8 I will not eat or drink while using computers.

3.9 I will never knowingly bring a computer virus, spyware or malware into school

3.10 If I think a school computer or a removable storage device that I am using contains a virus, spyware or other malware I will tell a member of staff

3.11 I will not open an attachment, or download a file unless I have permission or I know and trust the person who has sent it

3.12 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files

3.13 I will not attempt to log on as staff or an ICT administrator and understand that any attempt to do so will be dealt with severely. I am only permitted to log on as myself.

3.14 I will not attempt to connect to another pupil's laptop or device while at school. I am not permitted to establish my own computer network

3.15 I will not reply to spam emails as this will result in more spam. I will delete all spam emails

3.16 I will never attempt to install software on school computers or mobile devices myself.

3.17 I will not attempt to download software from the internet onto school computers

3.18 I will not knowingly install spyware or any sort of hacking software or device

3.19 I will try to prevent people from watching me enter passwords or viewing sensitive information

3.20 If I lose or misplace any portable ICT equipment I will inform a member of staff immediately.

4) Inappropriate Behaviour

4.1 I will not store, download or distribute music, video or image files on my personal user space unless they are appropriately licensed media files (e.g. Creative Commons licensed files) that I need for school

4.2 I will not use indecent, obscene, offensive or threatening language

4.3 I will not engage in personal, prejudicial or discriminatory attacks

4.4 I will not knowingly or recklessly send or post defamatory or malicious information about a person or about school

4.5 I will not post or send private information about another person

4.6 I understand that bullying, manipulation or exploitation of another person either by email, online or via texts will be treated with the highest severity and possible involvement of the school's designated Child Protection Officer, the Deputy Head (Pastoral).

4.7 I will not use the internet for gambling

4.8 I will not access material that is offensive or obscene, or that encourages illegal acts, violence or discrimination towards other people

4.9 If I mistakenly access such material I will inform my teacher or another member of staff immediately or I may be held responsible

4.10 If I am planning any activity which might risk breaking the Acceptable Use Policy (e.g. research into terrorism for a legitimate project), I will inform a member of staff beforehand to gain permission

4.11 I will not attempt to use proxy sites on the internet

4.12 I will not take a photo or video of another pupil or member of staff without their permission

4.13 I will not bring computer game files into school or store them on my personal user space and I will not play computer games in lessons without permission from my teacher

5) Monitoring

5.1 I understand that all files and emails on the school computer system are the property of the school. As such, system administrators and staff have the right to access them if required and I understand that the content of my Google Drive and school Google e-mail account is monitored, as are all e-mails that are sent or received, for offensive, inappropriate content, language, phrases and images.

5.2 I will not assume that any email sent on the internet is secure

5.3 I understand that all network access, web browsing and emails on the school system and laptops are logged and may be routinely monitored on any computer screen without the pupil's knowledge

5.4 I understand that if I am suspected of breaking this policy, my own personal laptop, storage device or mobile device can be searched by staff with the permission of my parents or carers.

5.5 I understand that the school reserves the right to randomly search the internet for inappropriate material posted by pupils and to act upon it.

6) Best practice

6.1 I will only print out work that I need as a paper copy – where possible I will use school systems such as email and Google Apps for Education to share information electronically.

6.2 I will not use school printing facilities to print non-school related materials (without prior permission).

6.3 I will not print on glossy paper, card or acetate on laser printers.

6.4 I will save work regularly using sensible file names

6.5 I will organise my files in a sensible manner and tidy my user space regularly

6.6 I will only use the approved, secure@qegsonline.com email system for any school communication

6.7 I will regularly back up any work that is not saved onto the school network

6.8 I will observe health and safety guidelines when using computer equipment

6.9 I will be considerate and polite to other users

6.10 When I leave school permanently, I will ensure that I save any files I wish to take with me as my account will be deleted

6.11 I understand that the use of music/video players, e.g. iPods, is banned during lessons unless I have permission from my teacher.

6.12 I will not connect music/video players to the school network, school computers or speakers without permission from my teacher.

6.13 I will only empty my recycle bin when I am certain I no longer need the files.

7) Social Networking

7.1 I will not load photos or videos of another pupil to website or social networking sites without their permission

7.2 I will not load photos or videos of a member of staff to websites or social networking sites

7.3 I will never access a member of staff's social networking profile or that of their friends and families.

7.4 I will never access social networking sites on school computers, unless instructed to do by a teacher for learning purposes

7.5 I will never create a bogus social networking account or site that is associated with a member of staff, pupils or the school.

7.6 If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, pupils or the school, I will inform a member of staff straight away.

7.7 I recognise that as an organisation, we do not use social networking sites to communicate with pupils, staff and parents (with the exception of our official Facebook and Twitter accounts).

7.8 When using Social Media sites I will BE POLITE. I will not send or encourage others to send abusive messages. I will respect the rights and beliefs of others.

8) Sanctions

8.1 If my actions cause damage to computer equipment, I will be charged for the cost of repairing items broken or damaged through carelessness or vandalism. Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

8.2 I may also be charged for the cost of correcting problems caused by hacking or tampering.

8.3 I understand that sanctions will vary depending on the severity of the offence, from a warning or withdrawal of internet use to suspension or exclusion. Any breach of the law may lead to the involvement of the Child Protection Officer and the Police.

9. Loss, Theft, and Damage

9.1 Queen Elizabeth's Grammar School accepts no responsibility for personal equipment brought onto the site.

Student Signature

I agree to abide by the above Acceptable Usage Policy.

Signature………………………….………….….………………. Date …………………….…………

Full Name ………………………………...................................……… (printed)

Authorised Signature (Parent / Guardian)

I have read this Acceptable Use Policy and explained the terms of this agreement to my son / daughter.

Signature………………………….....…………...……………..… Date ……………………..…………

Full Name ………………………………....……………………………….…… (printed)

Updated by Mrs CY Gammon: August 2017 Approved by Board of Governors: December 2017