ICT ACCEPTABLE USE and E-SAFETY POLICY
(Senior School)

(This document is available on the school website or on request)

Reviewed May 2018

This policy must be read in conjunction with other pastoral QEH policies, paying particular to regard to the *Safeguarding Policy* (including the Prevent Duty), the *Student Code of Conduct*, the *Anti-Bullying Policy* (including cyber bullying), the *Exclusion Policy* and the *Behaviour Policy*.
This policy is reviewed annually in June, though changes are made in the meantime as necessary.

Introduction

QEH ICT Technical Support Department, its resources and its staff are committed to providing an excellent service to staff and pupils. The facilities exist to support the aims and objectives of QEH and as such must be treated with respect at all times. In particular, the ICT Technical Support staff seek to support the acquisition of knowledge and skills and to support the development of initiative, confidence, independence, self-discipline and a strong sense of values.

This document defines the QEH policy in respect of the acceptable use of their information and communication (ICT) facilities and all pupils must make themselves familiar with this policy as violations may lead to disciplinary action.

Purpose

The ICT Department is responsible, on behalf of QEH, for providing a safe environment in which to learn and achieve educational objectives. In so doing, the ICT Technical Support Department will seek to provide a first-class service whilst at the same time minimising and containing potential risks to QEH and its members.

The purpose of this policy is therefore to state clearly both pupils' obligations in using these facilities and the ICT Technical Support Department's responsibility and authority in taking action of safeguard them.

Personal Responsibility

Pupils, staff and all other users of the ICT system must accept personal responsibility for using the ICT facilities with respect and in accordance with this policy. It is the responsibility of all pupils to report any misuse of the network to a staff member. Misuse may come in many forms but it may commonly be viewed as actively searching on the computer system for information on the internet which promotes:

Illegal Acts - for example child abuse images or terrorist content
Bullying - involving the repeated use of threat or coercion to abuse, intimidate or aggressively dominate others

Discrimination – material promoting the unjust or prejudicial treatment of people on the grounds of race, religion, age, gender, sexual orientation, disability or gender identity
Drugs or substance abuse - material promoting the illegal use of drugs or substances
Extremism –material promoting terrorism and terrorist ideologies, violence or intolerance, including calls for the death of members of the Armed Forces
Pornography – material displaying sexual acts or explicit images
Self-Harm – material promoting deliberate self-harm, including extreme weight loss, or suicide

Misuse of the network may also involve the deliberate streaming of large data files or any other practice which will deliberately slow down the network speed.

QEH make no warranties of any kind whether expressed or implied for the network service they are providing. QEH will not be responsible for any damages suffered whilst using the system, including loss of data as a result of delays, non-deliveries, mis-deliveries nor service interruptions caused by the system or elements of it, or your errors or omissions. Use of any information obtained via the network or other information systems is at your own risk. QEH specifically deny any responsibility for the accuracy of information obtained via its Internet services.

Policy Statements

General

It is the policy of QEH to:

- provide a working environment that encourages access to knowledge and sharing of information
- maintain ICT facilities for academic and administrative purposes, which provide access to their communities for local, national and international sources of information
- ensure that the security, safety and reputation of QEH and their members are protected from harm or the risk of exposure to extreme or illegal material through the use or misuse of ICT.

Software and Hardware

This policy covers the use of QEH's ICT networks and the Internet, irrespective of the means by which they are accessed. The policy applies to pupils who are using the following methods of access whilst working under the auspices of QEH:

- wired connections via a school machine
- wireless (Wi-Fi) connections
- cellular connections (3G / 4G) on their own device

QEH invests in a range of software and maintains this software to prevent unauthorised/inappropriate access to the Internet and to monitor email. Software is also used to detect viruses and to monitor and control the use of all computer facilities. It remains the responsibility of the pupil, however, to treat all resources, facilities and services with respect and to adhere to this policy.

Access to educational Internet-based games may be allowed with some discretion.
Pupils will ensure that such games are quiet, cause no disruption and contain suitable age-appropriate content. Strict priority is given to anyone wishing to complete schoolwork.

Pupils will not unplug, insert or disconnect any cabling relating to ICT equipment, nor interfere with projectors unless they have been given direct permission to do so.

Acceptable use

It is the policy of QEH that:

- the ICT facilities are provided in support of teaching and learning, research and administrative activities
- pupils are expected to conduct themselves in a responsible manner and respect the rights of others when using the facilities
- only designated pupils or those given permission are permitted to use the facilities.

Network Etiquette and Privacy

Rules for using the computer facilities / own devices include, but are not limited to the following:

- pupils will not post nor upload any information, pictures or video to any website/app (including video and photo sharing websites/apps) that may be deemed unsuitable, offensive or annoying to others. In addition, pupils agree neither to post nor upload any material which identifies QEH, its staff or its students from any device whether within QEH or elsewhere
- publishing documents or photographs relating to QEH or their pupils without express permission is prohibited
- pupils consent to access and review by the ICT Technical Support Department of all materials created, stored, retrieved sent or received using QEH's ICT resources
- pupils should use appropriate language in all communications
- pupils should keep personal data private (e.g. home address / telephone number).
- pupils should not use the facilities in any way that would disrupt the use of the service by others
- pupils should take care to avoid excess printing (be brief, proof read work for mistakes before printing, avoid printing entire articles if an extract is all that is needed etc.).
- pupils should remember that humour and satire can often be misinterpreted
- pupils must cite references for any facts which they state
- pupils should respect the rights and beliefs of others
- pupils should be polite

Security

All use of the QEH systems must be under their own username and password unless specifically directed otherwise by a member of staff. Pupils must remember to keep their password private and not to share it with friends. If a pupil thinks that someone else has access to their account they should change their password (Ctrl + Alt + Del) and inform their tutor.

If a pupil takes home any QEH owned property then they are responsible for it. It will be necessary to check home and personal insurance policies to ensure that the risks of damage or theft to the QEH's equipment are covered. It is important that pupils are aware of their own personal security when transporting expensive and 'desirable' equipment between home and school. This equipment should not be left unattended. Pupils should be discreet when travelling on public transport or walking to or from QEH.

Personal Use

QEH accepts that pupils will want to use the computer system for their personal use.
Provided that this use is occasional, reasonable and does not interfere with or detract from everyday work and commitments, it will normally be tolerated. Pupils are able to use the facilities in this way at lunch times and at break times as well as occasionally in lessons.
Personal use during lesson times must be directed by a member of staff.

Unacceptable Use

The ICT Technical Support Department will prohibit the use of its facilities when used intentionally in contravention of the principles outlined in this policy. The activities prohibited under this policy include (but are not restricted to) those listed below. Pupils must not:

i. cause the good name and reputation of QEH to be undermined

ii. deliberately access, create, store, download or transmit any material that QEH may deem to be threatening, defamatory, abusive, obscene, racist or otherwise offensive or access any age-restricted material classified above their actual age

iii. send or partake in unwanted email, chain letters, pyramid letters or similar schemes

iv. gain unauthorised access to facilities or services

v. behave in a way, or use the facilities in such a manner, that violates any other QEH policy

vi. pretend to be someone else or give false information about themselves

vii. transmit, store or download any material in violation of any UK or other national laws. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws

viii. engage in cyber bullying – the use of technology to tease, intimidate or threaten (see *Anti-Bullying Policy*)

ix. make malicious use of any instant messaging platform over the school network

x. connect their personal device to any switch or hub linked to the school wired network

xi. use any VPN/proxy sites. Use of such sites/networks will be considered a direct attempt to compromise the security of QEH's network and will result in disciplinary action

xii. overuse, hack or back up the school network or use it in such a way that would deliberately slow down access for other users, e.g. by streaming or downloading movies

xiii. create personal Wi-Fi hotspots and grant other pupils access to the internet

If pupils have any concerns during the school day, or at any other time, they must raise them immediately with an appropriate member of staff (Form Tutor, Head of Year or Deputy Head (Pastoral)). These may include:

- a concern that their network security has been compromised
- any worry that there has been attempt by someone older from outside QEH to contact them (e.g. grooming, trying to discover personal details, travel plans etc.)
- any accidental access to a restricted site or one which has inappropriate content

Prevention and investigation of misuse

QEH reserves the right to access all information held on its facilities, including monitoring and intercepting any system logs, web pages or email messages. This is for the purpose of preventing and detecting misuse. It is the policy of QEH to:

- promote its *Acceptable Use and E-Safety Policy* to all their members and provide advice on acceptable use when asked
- undertake regular audits of all Internet activity to ensure pupils adhere to the detail and the spirit of the Acceptable Use and E-Safety Policy
- take swift action against anyone found to be misusing QEH's ICT facilities
- If it is suspected that a pupil's personal device is being used in an unacceptable way whilst on the school site or away from the site on school business, including the use of their own cellular data access, a member of staff will confiscate the device and ask the permission of pupil to gain access in order to investigate. If the pupil refuses to give permission for the member of staff to gain access, the device will be held until the pupil's parents can be contacted so that device can be accessed in their presence. The full cooperation of the family is expected in these circumstances

A representative from the ICT Department attends a regular meeting with pastoral staff and a member of the Senior Management Team to monitor, review and advise on aspects of e-Safety within the school.

Health and Safety

QEH has a separate ICT Health and Safety Policy. By agreeing to this Acceptable Use Policy you agree to follow the Health and Safety rules which govern use of ICT facilities. In particular, if you have a medical condition such as epilepsy which may be affected by the use of computers then you must inform QEH and a member of the ICT Technical Support Department.
QEH cannot guarantee the safety of personal chargers which may be brought in to charge personal devices. As a result, it is the responsibility of pupils to ensure that their own devices are fully charged before they are brought into school. The use of personal chargers is forbidden on the School sites.

Occasionally, QEH will want to share information with parents relating to changes to this policy, new online threats or trends which may affect pupils etc. This will usually be done via the weekly email bulletin to parents.

Disciplinary Action

Any breach of the ICT Acceptable Use and E-Safety Policy requires appropriate action. Depending on the severity of the offence and at the discretion of the Head of ICT, Deputy Head Pastoral or Headmaster, one of the following will apply:

1. Temporary ban on internet or network use. The length of the ban will be dependent on severity of misuse
2. Confiscation of mobile device if necessary
3. Permanent ban on internet use
4. Permanent network ban
5. Normal school disciplinary action
6. Police involvement, where appropriate

These are examples of minor and major offences.

Minor Offence

- Loading programs which are not already installed on computers
- Using a "*work-only*" computer for other purposes
- Disturbing others
- Sending nuisance emails or messages
- Accessing or sending inappropriate material

Major Offence

- Logging on as someone else with the intention of gaining access while banned or trying to conceal your true identity
- Hacking or compromising the security of a computer or the network
- Accessing or sending offensive / obscene material
- Taking and /or publishing images of staff or pupils
- Cyber bullying
- Creating Wi-Fi hotspots for other pupils to access the internet

If a pupil has been banned from using a school computer, this should not be an excuse for unfinished work. If necessary, unfinished work should be hand-written.

Appendix 1

Pupil responsibilities when using the School network (a copy of this will be in the pupils' planners, in addition to cyber bullying awareness advice, from September 2016)

QEH has a high speed connection to the internet and the Internet Service Provider used by the school filters information in order to control access to the available sites. In providing access the school will take all reasonable precautions to ensure that the materials accessed are appropriate and suitable. The systems will record the access made to sites and attempts to access unsuitable sites is registered. Pupils must accept personal responsibility for using the Schools' ICT facilities and their own devices with respect and in accordance with this policy. It is the responsibility of the pupils to report any misuse to a member of staff.

The network and Internet access is provided for pupils to support their learning, conduct research and communicate with others. These facilities are provided on the understanding that pupils follow these guidelines:

- Pupils are responsible for good behaviour. Rules regarding respect for individuals (including anti-bullying rules, cyber bullying and the use of obscene or offensive language) apply whilst using computers.
- All pupils should look after ICT equipment as part of school property and should tell the appropriate staff member as soon as any faults or damage are discovered
- Pupils should not eat or drink or use aerosol sprays near ICT equipment as they may cause serious damage
- Pupils should not attempt to find any offensive or extremist material on-line. If inappropriate data or sites are discovered please tell a member of staff immediately.
- Taking or using images or recordings of students or staff without their permission is not allowed
- Another person's password must not be used and pupils must not attempt to access or use any network, email account, or data without permission.
- Passwords must be kept private. If pupils think someone knows their password they should change their password immediately.
- ICT hardware and software should not be reconfigured, changed or moved unless under supervision of an appropriate member of staff

Prevention and investigation of misuse and disciplinary action
QEH will monitor all data, information and activity on its computer systems for the purposes of prevention and investigation of misuse. Permission may also be requested to access a pupil's personal device should suspicion arise that it has been used in a way which contravenes the spirit of this policy. Disciplinary action may be taken against anyone found to be misusing the school's or their own ICT facilities. Pupils should ensure that their own devices are fully charged before bringing them into school. Personal chargers should not be used on the school site.

I have read and understand the information given about and I will carry out my responsibilities when using the school network.

Pupil Name /Form: ……

Pupil Signature: ……

Date: ……

Appendix 2

Cyber bullying
In addition to the advice given by QEH in our *Safeguarding Policy,* the *Anti-Bullying Policy* and the *Behaviour Policy* and in the homework diaries, the DfE has issued very helpful guidance on cyber bullying: *Cyber bullying: advice for Headteachers and school staff*, which also includes advice for parents and carers on cyber bullying.

The advice contained within this guidance is embedded in the school policy above, but of particular note to staff, parents and pupils would be the following sections:

- the safety and reporting tools for various social networking sites (p5 of the *Advice for Headteachers and staff*)
- the contact details for mobile phone providers (p6 of the *Advice for Headteachers and staff*)
- the Advice for Children (p3 of the *Advice for parents and carers*) reprinted below
- the information and links on social networking (p1 and 2 of the *Advice for parents and carers*)
- the information and links on social networking (p2 of the *Advice for parents and carers*)

Appendix 3

Advice for children
The following are some things that parents may wish to consider teaching their children about using the internet safely:

- Make sure you use the privacy settings
- Always respect others – be careful what you say online
- Be careful what pictures or videos you upload. Once a picture is shared online it cannot be taken back
- Only add people you know and trust to friends/followers lists online. When talking to strangers keep your personal information safe and location hidden
- Treat your password like your toothbrush – keep it to yourself and change it regularly
- Block the bully – learn how to block or report someone who is behaving badly
- Do not retaliate or reply to offending e-mails, text messages or online conversations
- Save the evidence. Always keep a copy of offending e-mails, text messages or a screenshot of online conversations and pass to a parent, a carer or a teacher
- Make sure you tell an adult you trust, for example, a parent, a carer, a teacher, or call a helpline like ChildLine on 08001111 in confidence
- Most social media services and other sites have a button you can click on to report bullying. Doing this can prevent a bully from targeting you and others in the future. Many services take bullying seriously and will either warn the individual or eliminate his or her account
- While you are on your mobile phone make sure you also pay attention to your surroundings

Appendix 4

Protocol for pupil use of school email

The school recognises that email is a useful tool for communication. All pupils have an individual email account which they are expected to use. There are certain expectations with regard to email outlined below.

- Please check your email at least once a day
- If required, respond to emails from staff within 24 hours
- Do not use school email for personal matters
- Emails to staff should be formal in tone – Dear Mr/Mrs…, regards etc.
- Do not expect immediate replies to emails sent after 5pm or at weekends
- If you are emailing staff for help with homework you still need to attempt the home work
- If you are emailing work, double check that you have correctly attached the document in the correct format and that your name is in the header of the document. Remember to include a brief message in the email.