ICT Acceptable User Policy

for

QES Sixth Form

Section 1: Introduction

Queen Elizabeth School is committed to the development of a safe, secure, happy community which balances the principles of inclusive learning and the maintenance of clearly understood parameters.

We have a clear set of values which is the basis of all we do and central to the Sixth Form Contract:

- Respecting the past and its traditions
- Working hard and doing your best
- Being decent to others
- Being polite, friendly and courteous
- Looking out for others
- Getting involved
- Respecting the environment
- Thinking of others less fortunate
- Remembering that life is about more than money and material things
- Encouraging global citizenship

E-safety underpinned these values and is a vital component to ensure the highest standards of care. In a constantly changing world all our judgements are based on reference to these values.

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

We believe you have a right of access to modern Information Communication Technology. However you must use it safely in accordance with school policies. Crucial to being a Sixth Form Student at QES is compliance with the Sixth Form Contract – any activities either counter to this contract or explicitly stated under 'forbidden' below, would result in disciplinary action.

It is everyone's responsibility to report any instance which might be a cause for concern.
If you are aware of somebody breaching the AUP you have a duty to report it to a member of staff.

Given the constant changes in technology new issues arise all the time. This policy doesn't attempt to list every possible issue but focuses on those of a particular relevance at the time of writing. The policy will be reviewed in light of any future developments. It has been written with Sixth Formers in mind, to enable the young people in our care to establish a value led approach to IT use which will help you as you move into Higher Education and into a professional workplace.

Terms used within this document

Acceptable

Examples of behaviour and practices acceptable in terms of ICT use.

Good Practice

Examples of behaviour and practices that promote good information security and help protect school data and systems.

Forbidden

This describes activities that will render the user liable to disciplinary action,

Acceptable

- Accessing school-related web sites in relation to school work.
- QES information technology and communication systems are provided for the purpose of completing work at school.
- Limited personal use. Students can use the e-mail system, internet and computer applications for limited personal use during breaks or outside school working hours.
- Communication in connection with school.

Good Practice

- Any images, material, software or files downloaded via the Internet to school may be used only in ways that are consistent with the related licenses or copyrights. All downloading of software must be completed by or with the permission of IT Support. If in doubt please consult IT Support.
- Use only your own User ID and password.
- Use only the applications which you have authorized access.
- You should protect yourself from potential unwanted attention from organised criminals by not disclosing personal details on the Internet (e.g. on social networking sites, blogging sites, forums etc.)
- Log off if you leave your workstation, or lock if you are leaving for a short break.
- Ensure strong passwords are used. (All passwords should contain letters and numbers)
- Change your passwords on a regular basis (once a term).
- Choose passwords not based upon dictionary words and are not easy to guess.
- Never write down or share your password.
- Avoid saving multiple copies of data and documents and perform regular housekeeping, deleting or archiving old e-mails and folders as appropriate.
- Never trust external e-mail from unknown sources, especially any with attachments. If in doubt, these should be deleted without opening/saving any attachments.
- Never assume that external e-mail is secure - others may intercept your message.
- Mail should be sent to specific recipients only.
- Only print the final draft of a document rather than multiple review copies. Always ensure you collect your prints from the printer.
- Report any faulty or broken equipment to a member of staff; do not attempt to fix it yourself.

Forbidden

- Posting school sensitive information including staff and student details or making reference to QES which brings the school into disrepute on the Internet (e.g. on social networking sites such as Facebook, blogging sites, Youtube, forums etc.)
- Making your password available for other people to use the Internet service on your behalf.
- Intentionally downloading any copyright material without the owner's written consent. A copy of the consent must be retained.
- Downloading software that can be run without installing and bringing it into school on a pen drive or transferring via WebDAV.
- Deliberately accessing sites containing pornographic, offensive or obscene material.
- Tying up large proportions of Internet resources on non-school related activity, to the detriment of genuine Internet use at any time. This includes:
    - leaving live Internet feeds open to collect news or sports results
    - downloading images, video or audio streams for non-school related purposes.
    - making repeated attempts to access web sites that have been blocked.
    - storing non-school related data (e.g. holiday photos) on any school computer systems, devices and media or storing any data that contains discriminatory, abusive, pornographic, obscene, illegal, offensive or potentially defamatory content.
    - changing any software security settings.
    - using another student's e-mail sign-on to circulate messages or hiding your identity in some way.
    - installing or modifying encryption or other security methods.
    - sending personal files with attachments to internal or external parties.
    - unauthorised sending or arranging to receive school-classified information and/or information relating to individuals
    - sending e-mails containing sensitive information about students or staff.
    - circulating any 'chain' e-mails.
    - sending non school e-mails to large numbers of people (i.e. spamming).
    - online gambling and soliciting for personal gain or profit is forbidden.
    - gaining or attempting to gain unauthorised access to school information, pupil/staff information or computer systems.
    - removing, tampering with, modifying or disabling any approved security software or settings, for example, anti-virus, firewall, and encryption.
    - the posting of school sensitive information to news groups and chat rooms in any instance.
    - sending or arranging to receive messages known to be infected, or containing files infected with a virus.
    - sending hoax messages.

- sending or intentionally receiving messages or images via telephony services that contain discriminatory, abusive, pornographic, obscene, illegal, offensive or potentially defamatory content.
- sending or intentionally receiving any images of members of the school without prior permission.
- deliberately tampering with, or damaging school IT equipment.
- attempting to access the school wired network using your own device
- attempting to connect your own device to the school wireless network without permission
- accessing, or attempting to access, resources with an account other than your own