ICT Acceptable Use Policy

for

Pupils wishing to use their own laptop computer or tablet device to support learning whilst at school

Section 1: Introduction

Some pupils who have recognised and identifiable learning difficulties (eg Dyspraxia, Dyslexia) have great difficulty with some of the core literacy tasks required for the accurate recording and presentation of written work. For these pupils, the use of a laptop computer or tablet device, such as an iPad, to record work in class and at home can have significant benefits. Many pupils are significantly quicker at typing than handwriting. For some pupils, using ICT removes many of the barriers that learning difficulties put up.

The gradual introduction of ICT into classrooms alongside pupils using traditional methods, does however present challenges to the QES community. For this reason the Learning Support Department (in conjunction with other colleagues within school) has drawn up an *ICT Acceptable User Policy*. The aim of the policy is to provide pupils and parents with clear guidance and support. Alongside this policy, the Learning Support Department will train, support and closely monitor pupils with learning difficulties who it has been agreed can use a laptop or tablet in class.

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:

- 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 underpins 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 pupils have a right of access to modern Information Communication Technology. However ICT must only be used safely in accordance with school policies.

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.

Terms used within this document

Acceptable

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

- 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

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

- 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 for 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 (no blanket emails)

- 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

This describes activities that will render the user liable to disciplinary actio

- 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

Security

In no circumstances can QES be held responsible for the loss, damage or theft of any private ICT hard ware. It is the pupil's responsibility to take care of their device. Never leave it unattended around school, make sure you have a suitable protective case and do not let anyone else use it. You may leave your device in the Learning Support Office or at the main school reception when not in use.

Saving and printing work

You will not be able to access the full school ICT network with your own device; you will therefore need to be very well organised in saving your work. There are various ways you can save your work to the network; Miss Humpage will be able to advise you about this.

Classroom IT Etiquette

- Please speak to your teachers to discuss why and how you are using a laptop or tablet.
- It is your responsibility to print your work and either stick it in your book, or pass it on to your teacher (please do not email and expect your teacher to print your work).

- Ensure that your device is fully charged so that you do not need to move seats to plug in and charge up.
- Be discrete; do not create a fuss, do not distract or delay others.
- Make sure that you know how to use any application or programme you might use in school.
- Remember that ICT is not the answer to all difficulties. It is often just as easy and much quicker to use traditional methods, especially for diagrams, graphs etc.
- Inappropriate use of your device may mean that you may no longer be able to use it in school.

Permission

Before you will be allowed to use your device in class you will need to meet with a member of Learning Support Staff. They will provide training, advice and support in the use of ICT in class. You and your parents will also need to sign the *ICT Acceptable User Policy* to demonstrate that you understand and agree to abide by it.

In order to gain wireless access to the internet I agree to abide by the terms outlined in this document.

Name of student: …… Form: ……..

Signature: …… Date: …….

Name of parent: ……

Signature: …… Date: …….

Please take this slip to Learning Support who will liaise with IT Support in order to obtain wireless access to the internet.