Review date: Annual review
Review officer: Head of ICT, School Counsellor and Academic Principal

E-Safety Policy

Rationale

New technologies are integral to the lives of adults, teenagers and younger children in today's society, both inside school and in their lives outside.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Students are always entitled to safe internet access.

The requirement to ensure that students can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our E-Safety Policy will help to ensure safe and appropriate use. The implementation of this policy needs to involve all the stakeholders in a child's education from the head teachers and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

QIS requires that all users of the internet abide by this policy as well as any local and international laws that relate to online child protection, family rights, stalking or harassment and hacking.

Aims

The aim of this policy is to guide students (and their parents / carers), staff and other users of our systems and equipment to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The use of technology can put students at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- The loss and / or damage to personal data.

• The potential for excessive use, which may impact on the social and emotional development and learning of the young person.

The use of technology can put students at risk within and outside the school. Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is used in conjunction with other school policies (eg. Safe Guarding Policy).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

This policy will also be used to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place in or out of school.

Procedures

1. Data protection, safety and personal privacy

1.1 Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

• At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and other devices, ensuring that they are properly logged-off at the end of any session in which they are using personal data.

•Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

• Data must be encrypted and password protected.

• The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).

• The device must offer approved virus and malware checking software.

• The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

1.2 Safety – use of digital images (including video footage)

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupil's instant use of images / footage they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

• When using digital images, staff should inform and educate students about the risks associated with their taking, use, sharing, publication and distribution. They should recognise the risks attached to publishing their own images on the internet eg. on social networking sites.

• Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Students must not take, use, share, publish or distribute images of others without their permission.

• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of students are published on the school website.

• Student's work can only be published with the permission of the student and parents or carers.

1.3 Personal privacy

Staff and students have a responsibility to ensure their personal information online is protected to prevent others from using this information to access your details or impersonate you. Measures to protecting your privacy should include:

• Stop and think before you share any personal or financial information - about you, your friends or family. Don't disclose identity information (drivers licence, birth date, address) through email or online unless you have initiated the contact and you know the other person involved.

• If you use social networking sites, adjust your privacy settings to control the amount and type of information you want to share, so that people you don't know very well can only see certain parts of your profile.

• Don't give your email address out without needing to. Think about why you are providing it, what the benefit is for you and whether it will mean you are sent emails you don't want.

• Before giving your email address online read the website privacy policy. This should tell you how they will use the email address you provide.

• If you often use your email address online you may want to have a secondary email account. Use your primary email with friends and businesses you know and trust.

• Set strong passwords, particularly for important online accounts and change them regularly-consider making a diary entry to remind yourself.

2. Computer misuse

2.1 Teaching and support staff

• Are responsible for ensuring that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

• They report any suspected misuse or problem to the Head of ICT or Head of Year for investigation / action / sanction.

• Digital communications with students (email / ClassDojo / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems. Teachers are not permitted to enter into text messages or any groups such as WhatsApp with students or parents.

• E-safety issues are embedded in all aspects of the curriculum and other school activities.

• Students understand and follow the school e-safety and acceptable use policy.

• Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• They monitor ICT activity in lessons, extra -curricular and extended school activities.

• They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

• In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

2.2 Students

• Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign (by a parent/carer) before being given access to school systems.

• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying. (Cyber-bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature).

• Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

• Should refrain from any online activity that is outside of school hours, which may have a negative impact within the school environment.

2.3 Parents/carers

Parents/carers play a crucial role in ensuring their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

• Endorsing (by signature) the Student Acceptable Use Policy.

• Accessing the school website / VLE / online student records in accordance with the relevant school Acceptable Use Policy.

2.4 Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

• School ICT systems will be managed in ways that ensure the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy.

• There will be regular reviews and audits of the safety and security of school ICT systems.

• Servers, wireless systems and cabling must be securely located and physical access restricted.

• All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Network Manager.

• All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password regularly.

• Users will be made responsible for the security of their username and password; they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

• The school maintains and supports the managed filtering service. The school has provided enhanced user-level filtering.

• In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the relevant Head teacher (or other nominated senior leader).

• Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Principal. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

• School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

• An appropriate system is in place (to be described) for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

• The school infrastructure and individual workstations are protected by up to date virus software.

• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

3. Social networking etiquette

Social network etiquette is required when communicating and interacting on the internet. The following net etiquette rules must be followed:

• Never use threatening, defamatory, nasty or foul language when communicating online.

• Do not respond to rude or threatening messages whether in chat, forums, comments or message boards.

• Always leave if the conversation makes you uncomfortable.

• Do not engage in 'flaming' – i.e. an online battle of aggression or insults between two or more people.

• Do not send emails IN ALL CAPS – it's considered to be shouting. • You must not say nasty or untrue things about others especially in public forums, newsgroups, or chat. These remain in many archives and you could be accused of libel, defamation or slander.

• Never forward personal emails sent to you to others without checking with the original sender first.

• Similarly, when forwarding an email to others, respect the privacy of your group of friends or family. Do not publicly broadcast all their email addresses, use the BCC command to keep them private.

4. Reporting antisocial/illegal online behaviour

4.1 Illegal behaviour

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

• Child sexual abuse images.

• Adult material which potentially breaches the Obscene Publications Act.

• Criminally racist material.

• Other criminal conduct, activity or materials.

You must:

• If you have actual evidence, disconnect the computer (if possible) from the mains immediately but do not delete any evidence.

• If you are confident that the Network Manager is not involved, speak to them immediately. Otherwise do not involve them and speak to the Head of Primary or Secondary.

• The local authorities may need to become involved at the decision of the Academic Principal.

4.2 Antisocial, legal behaviour

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedure.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place in or out of school. Inappropriate e-safety behaviour relating to QIS staff will be dealt with on a case-by-case basis.

While on site, students may receive a form of disciplinary action and/or warning letter (Level 4 Sanction) for any of the following example issues:

• Unauthorised access to/loss of/sharing of personal information.

• The deliberate introduction of a virus to the school network.

• Use of the personal data of other students.

• Uploading inappropriate materials (games, images, bad language etc.)

onto the network.

• Cyberbullying.

• Inappropriate use of personal digital devices such as mobile phones and tablets.

• Cheating, copyright and plagiarism.

• Accessing restricted or inappropriate online content.

• Access to illegal, harmful or inappropriate images or other content.

• Sharing / distribution of personal images without an individual's consent or knowledge.

• Illegal downloading of music or video files.

• Use of unlicensed / unofficial software within school.

• Inappropriate anonymous communication with peers.

- Out of school online activity that may have negative repercussions within school.

Evaluation

We live in a digital world where change is rapid – so much so that emerging technologies are sometimes hard to keep up with. With that in mind, our laws and sanctions must be constantly revised and updated.

There may be, inevitably, times where policies include certain 'grey areas' or do not address certain immediate or short-term changes to the way that new technologies are used. With that in mind, we all have a responsibility to approach these resources with a mature and responsible attitude; to monitor students so that they may be safe to enjoy and gain positive experiences from their online activities; and to conduct ourselves in a way that models these standards at all times.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date has been provided at the beginning of the policy.