



E-safety and ICT Acceptable Use Policy

Rationale

As a School working with our local, national and international communities, ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Streaming videos and music
- Gaming
- Mobile/Smart phones
- Other mobile devices with web functionality

Whilst beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At King Edward's School, we understand the responsibility to educate our pupils on E-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Policy are inclusive of both fixed and mobile internet; technologies provided by the School (such as PCs, laptops, webcams, whiteboards, digital video equipment); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, tablets).

Roles and responsibilities

As E-safety is an important aspect of strategic leadership within the school the Head has ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The Deputy Head and the Director of ICT have the responsibility of ensuring the policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance.

This policy, supported by the school's Acceptable Use Policy is to protect the interests and safety of the whole school community.

E-safety skills development for staff

- Staff receive regular information and training on E-safety issues in the form of INSET sessions.
- New staff receive information on the School's Acceptable Use Policy as part of their induction.

Communicating the School's E-safety messages

- E-safety has a prominent part in the 1st to 3rd Form Computing curriculum and is included in all new pupil inductions.
- Pupils are informed that network and Internet use will be monitored.
- External speakers speak to all year groups on a regular basis to highlight the importance of e safety.
- Parents are invited to E-safety talks and the subject is also talked about in the Moving to the 3rd Form event.
- Visitors are reminded of the School's expectations for acceptable use of electronic devices, whilst they are on the School's premises.

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. We regularly monitor and assess our pupils' understanding of E-safety.

- The School provides opportunities within a range of curriculum areas and discrete Computing lessons to teach about E-safety in accordance with the medium term planning.
- Educating pupils on the dangers of technologies that may be encountered outside school may also be done informally when opportunities arise.

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information and images, through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Pupils are taught to evaluate critically materials, and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

Password security

Password security is essential for all pupils and staff in the school, to ensure that the correct people have the correct access to the network. All users are reminded of the need to keep passwords confidential at their induction.

The schools enforces complex passwords. Valid passwords must be:

- At least 8 characters long
- Not contain parts of their name
- Be changed every 3 months

They must also contain 3 of the following:

- Lower case letters
- Upper case letters
- Numbers
- Punctuation

Data security

The accessing and appropriate use of school data are some things that the School takes very seriously. Staff are aware of their responsibility when accessing data through regular INSET sessions, including their responsibilities under the Data Protection Act. Level of access is determined by the Director of ICT.

Managing the internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- All users must read and agree to the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- All access to the internet is through a firewall and web filter.
- Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required.
- It is the responsibility of the school, by delegation to the technical support to ensure that Anti-virus protection is installed and kept up-to-date on all school machines. Bradford Campus Manger is used to ensure Antivirus protection is installed on BYOD laptops.

Social Networking Sites

Social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- Teachers should not become 'friends' with pupils on any social networking site.
- Staff and pupils should not share contact information on any social networking site.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/e-mail address, specific hobbies/interests).
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of bullying to the School.

Personal mobile devices (including phones)

- Internet content is filtered and firewalled
- Wifi access is limited at times, and some sites are time and age restricted
- Use of phones in lessons is not allowed without specific permission of the teacher
- In the Lower School, mobile usage is restricted to before and after school hours
- In the Senior School, the 3rd and 4th Form have been handing in technology overnight
- Mobile free zones are:-
 - Chapel at all times
 - Dining Hall at all times
 - Library during lesson times
 - Swimming pool area at all times
 - House day rooms between 08.10 and 08.30 and 18.30 and 19.00, at the time of the major roll calls
 - Between 08.40 and 10.50, 11.15 and 13.05 and 14.05 and 15.55 Monday to Friday outside the boarding houses, unless specifically agreed with a teacher
- Piccadilly Café will be a mobile friendly zone at all times

In the zones mentioned above, there will be a no see, no hear policy. This includes holding a phone, answering a call, looking at a screen and listening to anything through headphones. A separate mobile phone policy for the Lower School is attached at Appendix 1. Other rules may apply in the Senior School as determined by Housemasters and Housemistresses.

An immediate sanction will be issued for any infringement of the conditions that are outlined above.

Managing e-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. Educationally, e-mail can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. It is recognised that pupils need to understand how to style an e-mail in relation to their age and good etiquette.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- Staff should only e-mail pupils using their school e-mail address.
- All e-mails should be written carefully before sending, in the same way as a letter written on school headed paper.

Taking of images and film

Digital images are easy to capture, reproduce and publish and, therefore, misused. It must be remembered that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- Parents can request that images are not taken of their son/daughter. Before taking any image, it is important to check with the Marketing Department that permission has not been withdrawn.
- Any image taken should be transferred to the School's network and then deleted from any private device as soon as possible.

Misuse and Infringements

Complaints

- Complaints relating to E-safety should be made to the Director of ICT.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and must be reported to the Senior Lead Person.
- Pupils and parents will be informed of the complaints procedure.

Inappropriate material (see ICT Acceptable Use Policy)

- All users are aware of the procedures for reporting accidental access to inappropriate materials; the breach must be immediately reported to the Director of ICT.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Director of ICT and the School's sanctions policy will be followed.

- Users are made aware of sanctions relating to the misuse or misconduct. These sanctions could involve the withdrawal of access to the School's network or further sanctions in line with the School's Behaviour and Discipline Policy to match the needs of the offence.

Equal opportunities

Pupils with additional needs

The School endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the School's E-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-safety. Internet activities are planned and well managed for these children and young people.

Parental involvement

It is essential parents and carers are fully involved with promoting E-safety both in and outside of school. We regularly consult and discuss E-safety with parents and guardians and seek to promote a wide understanding of the benefits related to ICT and associated risks.

ICT Acceptable Use Policy

By using the computers, computer network or e-mail at King Edward's Witley, staff and pupils agree to abide by the terms of the Acceptable Use Policy outlined in this document and available on the School's intranet pages.

The computer network is owned by the School and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. This statement has been drawn up to protect all parties.

The School reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff and pupils using the School computer network and Internet are required to abide by this Acceptable Use Statement.

- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the School ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- In particular users are reminded of the danger in entering into e-mail correspondence with people whom they do not know.
- For privacy and security reasons Internet web pages will never include the full names of pupils.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials must be respected.
- All Internet activity should be appropriate to staff professional activity or the pupil's education.
- Legitimate private interests may be followed where these cause no difficulties for other users and do not compromise School use.
- The same professional levels of language and content should be applied to e-mails as for letters or other media, particularly as e-mail can be forwarded or may be sent inadvertently to the wrong person.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Users must access only those sites and materials relevant to their work in School or legitimate private interests.
- Users will be aware when they are accessing inappropriate materials and should expect to have their permission to use the system removed.

Privacy of school e-mail and school files on the School network

- It is possible for the Network Manager and Director of ICT to access all files on the School network. This allows the School to safeguard work and restore it where necessary.
- It is also theoretically possible for the Network Manager and Director of ICT to access all School e-mail. In reality this does not happen, unless there is a specific request from the Head or the Deputy Head.

The School monitors the network in a number of ways:

- The School uses a proxy server to filter the School's internet connection. As well as controlling which sites pupils and staff can visit, the device lists websites visited along with volumes of downloads and hours spent on the internet.
- The School also uses a device to filter the School's e-mail, attempting to remove viruses and other harmful material from entering or leaving our IT systems.
- Securus is installed on all desktops and School owned laptops. Securus monitors the use of these machines and obtains screenshots of any behaviour that it deems suspicious. It records behaviour under various categories, for example, bullying, pornography and bad language.

Use of external sites such as Facebook and non-School based webmail

- The School does not and cannot access private comments on any public e-mail or social networking sites such as Facebook or Hotmail.
- However, if such sites are accessed through a School owned computer which has Securus installed, and behaviour is exhibited which Securus finds suspicious, e.g. swearing, then Securus will obtain and record a screenshot which is then accessible to the Network Manager and Director of ICT.

Regulation of Investigatory Powers Act 2000

Ancillary to their provision of ICT facilities the Head asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

Appendix 1

Lower School Mobile Phone Policy

Rationale

The use of mobile phones by Lower School pupils during the working day is restricted to essential communication between the pupil and his/her parents/guardians. It is understood that pupils travelling to and from school on public transport should have the use of their mobile phone for safety reasons. All pupils in the Lower School have access to laptops in their spare time. These are connected to the School Wi-Fi and the School's E-Safety and ICT Acceptable Use Policy applies.

Procedures

With the above rationale in mind, the following practices are in place:

Day pupils

- All day pupils are to put their mobile phones into their allocated locker in Matron's office as soon as they arrive.
- If a day pupil needs to make contact with his/her parent/guardian during the school day, they can do so at break and/or lunch time, with the permission of the Matron on duty.
- Day pupils can collect their phone after their last activity has been completed, as they leave for home.

Boarding pupils

- Boarders have access to their mobile phones from 19:30 until 20:15. This time can be used to make contact with their family and friends. There are plenty of quiet places in QMH, allowing pupils to have appropriate privacy.
- Boarding pupils should return their mobile phones to their locker at 20:15. A check will be carried out by the duty member of staff during the bed time routine.
- As with day pupils, boarders may request use of their phones to communicate with their parents/guardians outside of this time slot.
- Mobile phones may be charged during the school day, in Matron's office. No charging is currently permitted overnight.

Accessible Content

The School operates an effective and comprehensive filtering system. Categories included in the blocked list includes social media. We understand that pupils can access social media sites through use of their own 3G/4G reception and staff are vigilant in their monitoring of this. It is expected that parents monitor their child's internet usage, to minimise the chance of inappropriate activity taking place.