Bassingbourn

Village College

Esafety and ICT Policy

October 2011

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 recognize 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
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and 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 Bassingbourn Village College, 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.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and our staff therefore have a shared responsibility to ensure that this could not be accessed by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school.

Everybody in the school, has a duty to secure any sensitive information used day to day and should be made aware of the risks and threats and how to minimise them, including staff not directly involved in data handling.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by

students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may look at any ICT equipment owned or leased by the School at any time without prior notice. ICT staff may monitor, intercept, access, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law.

This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any work related issues retained on that account. All monitoring, surveillance or investigative activities are conducted by ICT staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a School employee or contractor may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's E Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the school's eSafety Co-ordinator.

Computing Facilities

Students are encouraged to make use of the college computing facilities for educational purposes. All users are expected to act responsibly and show consideration to others.

Logging on and Security

- Students are responsible for the protection of their own network logon accounts and must not divulge passwords to anyone. Anyone who feels their password has been compromised should change it immediately.
- Passwords are best when they are complex (minimum of 6 characters and including numbers and upper and lower case letters).
- Students are forbidden to log on as someone else, nor use a computer which has been logged on by someone else.
- All students must either log off when leaving a workstation or lock the workstation, even for a short time.

Use of the Network and Computer facilities

It is not acceptable to:

- Play game on the college network (except at lunchtime under supervision in room 46)
- Attempt to download or install programmes to a computer based solely in the college.
- Attempt to introduce a virus, or malicious code.
- Attempt to bypass network and systems security
- Attempt to gain access to another user's account.
- Attempt to gain access to an unauthorised area or system.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- Engage in activities which waste technical support time and resources
- To fix, move or alter any aspect of hardware which is the jurisdiction of the ICT Support and development Team without prior arrangement.

Use of the Internet

Access to the Internet is filtered to prevent access to inappropriate sites, and to protect the computer systems. Students should be aware that the college logs all internet use for students and for staff.

- The use of public chat rooms or messaging services (such as MSN,AOL or ICQ) is not allowed.
- Students should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to a disqualification by examination boards.

- Students should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- The use of the internet during lessons is under the direction of the teacher.

Use of E Mail

Automated software scans all email, and removes anything which could affect the security of the computer systems, or contain unsuitable or offensive content.

- Students are not allowed to use email during lessons, unless the teacher for that lesson has allowed its use.
- Students may only use the e mail accounts set up by the college. The use of e mail facilities such as Hotmail, Yahoo and Googlemail is not permitted.

Use of Other Technologies

Technology such as media rich phones, MP3 players, Personal Digital Assistants (PDA), memory cards, USB Storage Keys and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with the safety and ICT Acceptable Use Policy even if not connected to the college network.

Specifically, it is an offence for mobile phones or computers to be used to record and /or transmit images or messages which are obscene or which contain threats or verbal abuse. This 'cyber bullying' is unacceptable, especially where it is directed towards another member of the college community.

Use of Instant Messaging

The use of Instant Messaging (IM) is not permitted within Bassingbourn Village College Network.

Social Networking

Students using Social networking sites outside of the school date e.g. Facebook, bebo, My Space must NOT:

- Attempt to contact members of the staff or invite them to be friends
- Post messages/create sites which are abusive in any way towards any other members of the College community.

Students are advised not to:

- Advertise your personal information
- Leave your profiles unlocked for entire communities to read
- Reveal which social networking site you use.

Printing

All printing within the college is logged by printer and by user

Privacy and Personal Protection

- Students must at all times respect the privacy of others.
- Students should not supply information about themselves, or any other member of the College Community, on websites, within email or instant messaging.
- Students must not attempt to arrange meetings with anyone met via websites, email or instant messaging
- Students should realize that the college has a right to access personal folders on the Network. Privacy will be respected unless there is reason to think that someone is not following the safety and ICT Acceptable Use Policy in which case they will be subject to disciplinary procedures.