city college | brighton and hove

E-Safety Policy

Policy	E-safety
Originated	April 2010
Lead Manager	Vice Principal Student and Learning Support
Reviewed by CLT	May 2011

E Safety Policy

1.0 Introduction

New technologies have become integral to the lives of children and young people in today's society, both within colleges and in their lives outside college. 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. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

However, colleges must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and protected from potential harm, both within and outside school. This approach is enshrined in our Safeguarding policy of which this document is an integral part.

This e-safety policy explains how we have done everything that could reasonably be expected to manage and reduce these risks. It also addresses the wider educational issues of how to help young people and our staff to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1.1 Scope of the Policy

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

The policy refers primarily to use of technology on college premises or for college related educational work or through communication channels that specifically link to the college. However, this policy may also apply to conduct by students or staff (such as incidents of cyber-bullying or other e-safety incidents covered by this policy) which take place out of college, but is linked to membership of the college and which impacts on the college community, individuals or reputation.

1.2 Risks faced

There are a wide range of risks and dangers that face young people which could impact on the safety or security of students. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.

- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- sharing of personal data which may allow:
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying

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.

2.0 Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the college:

2.1 Governors

Governors are responsible for the approval of the E-Safety policy and Safeguarding work of the college of which e-safety is an important part. A member of the Governing Body has taken on the role of Safeguarding Governor which will include:

- attendance at the Safeguarding working group
- evaluation of incidents including ones related to e-safety
- reporting to relevant Governors committee (Quality Committee)

2.2 The Senior Management Team

The Senior Management team is responsible for ensuring the safety (including e safety) of members of the college community. They will receive reports from the E-Safety Steering group (see below) and take appropriate actions as is appropriate and necessary,

2.2 E Safety Steering Group

The e-safety Steering group is made up of the Vice Principals for Student and Learning support and Teaching and Learning, the e-learning manager, the Head of IT and the Head of Intensive Support (Designated Child Protection and Safeguarding Manager). The group:

- takes responsibility for e-safety issues and has a leading role in establishing and reviewing the college e-safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- initiates training and advice for staff
- liaises with college ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

The group will meet termly and report to the Safeguarding Working group and contribute to the termly Safeguarding report to Senior Leadership Team and so to Governors.

2.3 Head of IT

The Head of IT is responsible for ensuring:

- that the college's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the college meets the e-safety technical requirements according JANET agreements
- That the college Acceptable Usage Policy meets the requirement of network security and user safety
- that users may only access the college's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the college's filtering policy is applied and updated on a regular basis
- that the use of the college network and Virtual Learning Environment (VLE), remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported
- that monitoring software / systems are implemented and updated as agreed in college policies

2.4 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that they:

- take responsibility for ensuring that students are e-safety aware and that students understand and follow the college e-safety and acceptable use policy

- take responsibility for the safe use by students of specified technologies which are part of teaching and learning
- complete training as required by the college
- have an up to date awareness of e-safety matters
- have read, understood the college E-safety and Staff IT Acceptable Use policy and
- report any suspected misuse or problem
- They monitor ICT activity in lessons, extra curricular and where appropriate extended college activities

2.5 Students

- Students are responsible for using the college ICT systems in accordance with the College Acceptable Use Agreement, which they will be expected to sign at induction
- 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 college policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand college policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of college and realise that the college's IT Acceptable Use Agreement covers their actions out of college, if related to their membership of the college

3.0 Acceptable Use

The college has an Acceptable Use Agreement for Students and an IT Acceptable Use Policy for staff. These documents aim to inform students and staff in relation to usage of the college IT systems of their responsibilities, what is acceptable and unacceptable use and consequences of misuse. They also help to ensure the security of the College IT Systems, to safeguard the college's business and reputation and to help provide a safe and appropriate teaching and learning environment for all College IT Users.

These documents are an integral part of this college e-Safety Policy. Breach of the agreement by students or the policy by staff can lead to formal Disciplinary procedures (see section 8.0)

The student Acceptable Use Agreement is at Appendix 1

4.0 Education and Training

4.1 Education and Training: Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the college's e-safety provision to help recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety session will be part of induction where they will discuss and sign up to the College Acceptable Use Agreement
- Students will be helped to understand the need for the student AUA and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside college

Key e-safety messages will be reinforced as part of curriculum delivery which will cover:

- the need to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- acknowledgement of the potentially serious impact of inappropriate use on the college and individuals
- how to report misuse that they observe or are subject to and how to receive appropriate support
- the need to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

4.2 Education and Training: Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned on-line e-safety training module is available to staff.
- All new staff will be informed of the need to complete e-safety training as part of their induction programme, ensuring that they fully understand the college e-Safety Policy and IT Acceptable Use Policies
- Staff will not be able to access selected sites or technologies for use in teaching and learning unless they have completed the training and received agreement from the E-Learning Manager

4.3 Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum. It is also recognised that

access to certain sites can enhance teaching and learning. The aim is to allow access to appropriate sites as needed for educational purposes whilst maintaining e-safety. To achieve this sites access to sites is determined by a traffic light system as determined by the filtering system Websense which is recognised as best provider and are classified as red, amber or green. The following process will apply.

- All can access green sites.
- Access to amber sites is only given when
    - the member of staff has completed the training and
    - they agree to take responsibility for the e-safety of their students with appropriate guidance and training and
    - with the agreement of the E-learning manager
- Access to red sites is normally not given unless in specific and particular circumstances and with agreement of the Vice Principal Teaching and Learning

5.0 Technical Infrastructure

The college will be responsible for ensuring that the college 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;

- College ICT systems will be managed in ways that ensure that the college meets required e-safety technical requirements
- There will be regular reviews and audits of the safety and security of college ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to college ICT systems.
- All users (at KS2 and above) will be provided with a username and password at enrolment. Users are required to update this
- Users will be made responsible for the security of their username and password, 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 college maintains and supports the managed filtering service provided by WebSense
- Requests from staff for sites to be removed from the filtered list will be considered by the e-Learning Manager and reviewed regularly by the E-Safety Steering group
- College ICT technical staff regularly monitor and record the activity of users on the college ICT systems and users are made aware of this in the Acceptable Use Agreement

- An appropriate system is in place for users to report any actual or potential e-safety incidents to the IT Manager

6.0 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff must ensure that they:

- At all times take care to ensure the safe keeping 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.

7.0 Responding to incidents

It is hoped that all members of the college 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.

When this occurs staff and students may be subject to disciplinary process. It is the responsibility of staff and students to report any apparent or actual incidents of misuse by students or staff which may include:

- Any behaviour by staff or students which affects the safety and security of the ICT systems or other users and is against Acceptable Use Agreement
- Any failings in technical safeguards which may become apparent when using the systems and services.
- Any incidents, messages or access to sites that make staff or students feel uncomfortable or unsafe
- Any damage or faults involving equipment or software, however this may have happened.

Misuse by students should be reported to the relevant team leader and will be dealt with through the college Managing Student Behaviour procedures.

Misuse by staff should be reported to the relevant College Manager

8.0 Disciplinary action

In the event of misuse, disciplinary action will be taken in line with the College's Staff Disciplinary policy and the Managing Student Behaviour Policy

Staff or students may lose access to the college network, be suspended from college or in the event of illegal activities, the involvement of the police

Where an incident involves members of the college community which may affect the reputation of the college or the professional standing of staff then disciplinary process may apply even if the member of staff or student is accessing or using technology outside college premises or on non college equipment

9.0 Monitoring Impact

The college will monitor the impact of the policy using:

- Logs of reported incidents
- WebSense monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Students (eg Ofsted “Tell-us” survey / CEOP ThinkUknow survey)
- Staff

10.0 Other Related Polices

- Safeguarding
- Full IT Policy
- IT Acceptable Use for Staff
- Equality and Diversity
- Staff Disciplinary

Appendix 1

IT Acceptable Use Agreement

Our computers and networks are a great resource that we want you to use to help with your studies and learning but you also have a responsibility to use the technology safely and responsibly. This acceptable use agreement tells you:

- How you can minimise any risks to yourself and others from misuse
- What you can and can't do when you are using the college network and computer technologies
- What to do if you want to report any concerns
- What the consequences will be if you do not follow this agreement

Personal safety

- I understand that I must use the college ICT and system and network in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems or other users.
- I have been made aware that there are risks associated with using computer networks which include:
    - Accessing illegal, harmful content such as games or web sites, images, videos or internet with inappropriate content
    - My personal information or images being used or shared without my knowledge or consent
    - Communication or contact with others, including strangers who may be dishonest about their intentions
    - Cyber-bullying by other students or people outside the college
    - Using the internet excessively which could impact on my social and emotional development
- I will actively take part in sessions on e-safety and follow instructions from my teachers or other members of staff
- I know that the college will monitor my use of the ICT systems, email and other digital communications.
- I will not share username and password or try to use any other person's username and password.
- I will disclose or share only essential personal information about myself or others when on-line
- I will immediately report to my Tutor, Team leader or Student Support any unpleasant or inappropriate material or messages, anything that makes me feel uncomfortable or if I feel I am being bullied

Security of the technology

- I understand that the college ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use
- I will not try to make excessive downloads or uploads that take up internet capacity and which may prevent other users from being able to carry out their work, unless previously agreed with ITSU by my tutor.

- I will not use the college ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, or try to use programmes or software to bypass the filtering and security systems in place
- I will not open any attachments to emails, unless I know and trust the person or organisation who sent the email, as it may contain viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use social networking sites with permission and at times that are allowed

Respect

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not use the technology in any way that may harm the reputation of the college or brings the college into disrepute
- I will not use the technology for cyber-bullying which includes sending offensive messages, posting offensive images or harassing others
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will not take or distribute images of anyone without their permission.

Copyright and Plagiarism

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- If I use materials from sources on the internet I will also acknowledge and reference the source in any written work or presentations

Reporting: I will immediately report to **my personal tutor, team leader or Student Support**

- any behaviour by other students which affects the safety and security of the ICT systems or other users and is against Acceptable Use Agreement
- Any incidents including communications from outside the college that make me feel uncomfortable or unsafe
- any damage or faults involving equipment or software, however this may have happened.

You can click on the STOP IT logo on Moodle or the intranet to directly report any incidents or concerns to Student Support

Consequences: I understand that I am responsible for my actions both in and out of college

- If I do not follow this Acceptable Use Agreement and am involved in incidents of inappropriate behaviour, I will be subject to disciplinary action as in the college Managing Student Behaviour policy.

- This may also apply if I am out of college and where the inappropriate behaviour involves members of the college for example cyber-bullying, use of images or personal information or harms the reputation of the college
- I understand that I then may lose access to the college network, be suspended from college and in the event of illegal activities involvement of the police

I have read and follow this Acceptable Use Agreement (signature)

_____