Colchester Institute

Learner e-Safety Policy

February 2013

Impact assessed: December 2012

Learner e-Safety policy

1. Introduction

Colchester Institute has a duty to safeguard and promote the welfare of its learners and this includes ensuring that they develop and apply their IT capability effectively and responsibly while studying at College.

It is the duty of the College to ensure that every child and young person in their care is safe and the same principles should apply to the 'virtual' or digital world learners will encounter whenever they use IT in all its various forms whilst studying at College.

The aim of this policy is to protect learners when using e-technology and the College IT systems during their time at Colchester Institute and to minimise risks and deal with any infringements.

2. The Technologies

IT has an all-encompassing role within the lives of children, young people and adults. New technologies enhance communication and aid the sharing of information. Current and emerging technologies used in and outside of college by children, young people and adults include:

- the internet
- e-mail
- Instant messaging often using simple web cams
- Blogs
- Podcasting (audio/video broadcasts either live or downloaded to computer or MP3/4 player)
- Social networking sites
- Video sharing sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'
- Smart phones with e-mail, web functionality and cut down 'Office' applications
- Micro-blogging sites (e.g. Twitter)
- Location based services (services that allow you to check in your current location so it is publicly viewable)
- iPads and tablet computers

3. Colchester Institute's approach to the safe use of IT

e-Safety is a component part of the College's commitment to the safeguarding of learners. Creating a safe IT learning environment consists of three main elements :

- Policies and procedures, with clear roles and responsibilities
- An effective range of infrastructure and technology
- e-Safety communications and training

4. Roles and Responsibilities

The senior leadership and management team (SLMT) recognise that e-safety is an essential aspect of strategic leadership and will aim to embed safe practices into the culture of the College. They are responsible for ensuring that the e-Safety policy is implemented and compliance monitored.

Managers are responsible for ensuring that the e-safety policy is implemented in their areas of responsibility and that policies, procedures and practices encompass safe use of technology and related systems.

All teaching staff are responsible for promoting and supporting safe behaviour in their classrooms and following the College's e-Safety policy.

Staff in IT Services are responsible for ensuring that the College IT systems and infrastructure are secure and include technology to minimise abuse/ misuse and monitor use by learners and staff. Such systems include:

- Web filters to protect against accessing inappropriate materials on the internet
- e-mail filters to protect against receiving inappropriate e-mails
- Anti-virus systems that provide virus/malware protection to PCs and protect users from uploading or downloading potentially unsafe files
- Firewall and other security systems to prevent hacking of the college IT facilities from external sources and to stop internal users from making unsafe connections from un-trusted sources.

5. Learner Acceptable Use Agreement

The college recognises that new technologies have become integral to the lives of children and young people in today's society, both within the College and in their lives outside College. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

 Whilst the College will ensure that IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk, learners are required to be responsible and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Learners will be required to agree to use communications technology and the College IT systems responsibly, to ensure that there is no risk to their own safety and security of IT systems and other users by signing that they have received and agreed the Acceptable Use Agreement at the point of course offer or enrolment, as shown in the Appendix.

Learners and staff will only be allowed access to Colchester Institute computer network when they have agreed to abide by Colchester Institutes Code of Practice for the use of Information Technology and e-Safety policy.

6. Communications and training

In addition to accepting the Acceptable use Agreement, learners will have access to the e-Safety policy through the College internet and other documentation provided prior to starting their course, such as prospectuses and learner handbooks.

e-safety will be included at learner induction, to raise the awareness and importance of the safe and responsible use of new technologies.

e-Safety will also be incorporated within the tutorial programme.

Teaching staff will remind learners of the rules and risks of safe use, at the beginning of any lesson using the internet or IT.

Staff will have access to the e-Safety and related policies through the College intranet site.

Training materials and programmes will be developed as appropriate, to enable staff to engage with IT in a safe manner.

If a member of staff is concerned about any aspect of their IT use in College, they must discuss this with their line manager.

7. Monitoring e-Safety, complaints and concerns

Though the College will take all reasonable precautions to ensure e-Safety, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a College computer or mobile device. Having taken all reasonable security precautions the College cannot accept liability for material accessed, or any consequences of internet access.

The Acceptable Use Agreement outlines the rights and responsibilities of learners, gives information about what constitutes an infringement and documents the range of sanctions that could be applied. These may include;

- interview or counselling by tutor, Curriculum Manager or Head of Centre
- loss of access to the College network / internet for a period of time
- contact with parents or carers
- action taken through the discipline procedure which could result in suspension and exclusion
- referral to the police

Learners who have concerns about e-safety can raise these with their course tutor or a safeguarding officer under the College's Safeguarding and Child Protection policy.

Staff who have issues or concerns about e-safety can raise these with their line manager or with Human Resources.

8. Associated Polices.

- Use of Social Networking and Web Services
- Code of practice for the use of Information Technology
- Data Protection Policy
- Safeguarding and child protection policy

Learner e-Safety Acceptable Use Agreement

This e-Safety Acceptable Use Agreement forms part of the Colchester Institute Learner e-Safety policy which is available on the Child Protection and Safeguarding Learners page of the Portal.

When you are offered a place or enrol on a Colchester Institute course, you must accept that you have read, understood and agreed to the rules included in the e-Safety Acceptable Use Agreement. If you do not accept this Agreement, access will not be granted to College IT systems.

1. I understand that the College will monitor my use of College computer systems and networks including wireless (WiFi), the Moodle VLE and the Portal.
2. I will keep my logins, IDs and passwords secret.
3. When I am communicating on-line I will be aware that people are not always who they claim.
4. If I am under 18 and arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
5. I will not disclose or share personal information about myself or others when on-line.
6. I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
7. If I use the computer for personal or recreational use I will make sure I am not preventing others from using it for educational use.
8. I will not try to make large downloads or uploads that might take up internet capacity unless this is part of my course.
9. I will not use the College computers or the wireless provision (WiFi) for on-line gaming, gambling, shopping, file sharing, or video broadcasting unless this is part of my course.
10. I will respect others' work and property and will not access, copy, remove or alter any other user's files.
11. I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language.
12. I will not take or distribute images of anyone without their permission.
13. I will only use my personal mobile phones / USB devices etc in College when appropriate and won't disrupt or offend others.
14. I will not upload, download or access any materials which are illegal or inappropriate.
15. I will immediately report any damage or faults involving equipment or software.
16. I will not open any attachments unless I know and trust the organisation or person who sent the email.
17. I will not install or attempt to install programs of any type, or store programs on a computer, nor will I try to alter computer settings unless this is part of my course.
18. I will only use chat and social networking sites at an appropriate time and place.
19. I will ensure that I have permission to use the original work of others in my own work and acknowledge the use of that work as appropriate.
20. Where work is protected by copyright, I will not download copies.
21. I will take care to check that the information that I access is accurate.
22. I understand that the College has the right to take action against me if I am involved in incidents of inappropriate behaviour when I am out of College and where they involve my membership of the College community.
23. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.