ILT E-Safety & ILT Code of Conduct Policy for Learners

Owner:	Director of ILT
CE Sponsor:	EVP: Finance & Corporate Development
Issue Date:	September 2021
Review Date:	November 2024
Approval date:	23 November 2021

ILT E-safety Policy - Social Media, Email, Networking

Introduction

IT enables almost everything that we do in College, whether this is learner, tutor, support staff or governor. It is integral in the day-to-day running of the College and the curriculum we deliver to our learners. It is vital that all parties are aware of the safeguarding issues surrounding the use of IT.

E-safety relates to the safe and responsible use of IT including computers, the internet, mobile devices and technological tools that are designed to hold, share or receive information. Examples include mobile phones, digital cameras, tablets and so on. Learners and staff need to use technology in a safe and responsible way; demonstrating appropriate online behaviour.

To this end all learners, governors and staff of the College are required to sign an Acceptable Use Policy, which lays out the terms and conditions for the use of ILT within the College to ensure that all members of the College community are kept safe, and are aware of their responsibilities.

Related Policies

- Acceptable Use Policy

Aims of IT and mobile devices

We are committed to using the internet and other digital technologies and devices to:

- Make lessons more varied, rich, exciting and interactive and so raise educational standards enable learners to gain access to a wide variety of knowledge in a safe way
- Prepare learners for using the internet safely outside of College and throughout their education

Benefits of the policy:

- Assist in protecting learners, governors, staff and College systems
- Ensuring integrity of information and in improving processes by enabling certain controls which are essential to safeguarding in our role as guardians.
- Providing a productive and safe learning environment
- Assist College staff working with learners to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Minimise the risk of misplaced or malicious allegations made against staff who work with learners.
- Ensure that all members of the College community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Embed the importance for the long term implications of any content posted online
- Emphasising good practice in keeping personal information safe

Communication

The policy will be communicated to learners, staff and governors in the following ways:

- Policy to be posted on the College website, the College policies site (the portal) and website
- Policy to be part of College induction pack for new students
- Acceptable use agreements discussed with learners at the start of each year.
- Acceptable use agreements to be issued to whole College community, usually on entry to the College
- Acceptable use agreements to be held in learner and personnel files

Evaluation and Review

This policy will be monitored through College self-evaluation processes and will be reviewed by the College executive. The policy will be reviewed every three years or when a significant change in technology occurs to ensure that the content remains current and up-to-date with technological and e-safety developments.

ILT CODE OF CONDUCT AT COLCHESTER INSTITUTE FOR LEARNERS

All learners must take responsibility for their own actions when using the College's internet and email system, and must exercise care and consideration at all times. All learners must follow the conditions described in the policy when using College ILT mobile and networked resources including GSuite both inside and outside the College. Learners will be provided with guidance by staff in the use of resources available. College staff will regularly monitor the network to make sure that it is being used responsibly. The College will not be responsible for any loss of data because of system failures or learner mistakes in using the system.

Conditions of Use

Learners will be expected to use the resources for the educational purposes for which they are provided. It is the personal responsibility of every learner to take all reasonable steps to make sure they follow the conditions set out in this policy. Learners must also accept personal responsibility for reporting any misuse of the network.

Definition of technology

The definition of technology includes, but is not limited to, computers, laptops, netbooks, Chromebook, iPads, tablets, iPod Touch, collaboration tools, internet technologies, wearable technologies and any mobile devices.

Personal devices

Personal devices brought into College are entirely at the learner's own risk. The College accepts no responsibility for the loss, theft or damage of any personal device brought into College. The recording, taking and sharing of images, video and audio on any personal device is to be avoided and should not be undertaken without the prior consent of the person or people concerned. Learners need to be responsible for protecting their own personal information held on these devices including their phone number for example. Personal devices may be used during lessons at the request of the teacher if this supports learning and teaching; otherwise all personal devices should be on silent and kept out of sight during lessons, and will be confiscated if not. The Bluetooth or similar function should be switched off and may not be used to send images, files, audio or video to other personal devices. Bullying via any personal device will be addressed in accordance with the relevant College policies on bullying.

Internet filtering

The College uses an educational filter which filters the internet available through our network for all learners, staff and governors who have access whilst on site. The College will maintain a list of inappropriate and banned terms; the use of these in emails will be detected and logged and access will be denied via the internet. The College will ensure filtering systems are appropriate, efficient, and as effective as possible. This will entail regular checks and ongoing monitoring. Web Filtering is managed by ILT, who are responsible for ensuring that filtering is current and respond to requests for unblocking site in line with curriculum needs. Chat rooms, social media sites and web cam sites are disabled to ensure that learners remain safe. The ILT team may run reports at any time where a member of staff or learner has raised concerns about sites being viewed. If a learner discovers an unsuitable site, the URL, time and date must be reported to ILT, so that action can be taken.

Virus protection

The College maintains a current and regularly updated antivirus system. The system is configured to prevent exe files from running and prevents zip files being emailed to maintain a healthy network.

Social networking including social media

Social networking is a part of everyday life. Learners are encouraged to follow the age restrictions on social media sites. Learners should not seek to add or friend members of staff or their friends and family. Nor should this be a platform for anti-social behaviour towards other learners. Social media sites should not be accessed during lessons on personal mobile devices unless specifically directed by a staff member, and cannot be accessed on College held devices. The College does have social media accounts which are College related and learners are encouraged to join these forums when appropriate.

GSuite

When users sign into GSuite for the first time they are prompted to accept the GSuite acceptable use policy. This policy states that Google is in charge of the security of the user's data but users are in charge of the legality of the data created/uploaded. Any data that is uploaded to Google that breaches UK Law e.g. Copyright Infringement, renders the individual user liable. Google also enforces a strong password policy. The College network administrators carry out spot checks on learners GSuite accounts to check for misuse. All users will be mindful of copyright issues and will only upload appropriate content. When staff or learners leave the College their account or rights to specific College areas will be disabled or transferred to their new establishment.

Password policy

Learners are required to reset their passwords regularly. A password policy enforces the use of strong passwords by using symbols, uppercase, lower case and numbers. The password is private and must not be shared with other learners or left in a place where it is vulnerable to detection. Any misuse of a learner account due to password sharing will lead to further investigation and possible sanctions.

Digital images and video

Learners are taught via the e-safety programmes and assemblies about the use of digital images and videos. Learners are taught the risks associated with a digital footprint and providing information online. Learners should not take images or videos of other learners unless prior permission has been given by the learner. Images or video should only be taken in College for educational purposes. Under no circumstances should a learner take an image or video of a member of staff on a personal device without that staff member's express and individual consent

College website

Photographs published on the website will be carefully selected and comply with good practice. This includes:

- Not using learners' full names particularly in association with photographs
- Written permission is obtained before photographs are used on the website.

Cyberbullying

The College believes that everyone in the College community has the right to learn and teach in a healthy and caring environment without fear of being bullied. We are committed to educating learners and parents about cyberbullying and its potential consequences. Cyberbullying is the use of ILT to deliberately upset someone else. It can include threats, intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images. It can include messages intended as jokes, but which are harmful or upsetting to another learner. Cyberbullying may be different to other forms of bullying in the following ways:

Impact: possibly extensive in scale and scope

Location: the anytime and anywhere nature of cyberbullying

- Anonymity: the person being bullied might not know who the perpetrator is

Motivation: the perpetrator might not realise that his/her actions are bullying Evidence: the subject of the bullying will have evidence of what has happened

Cyberbullying is considered as serious as any other form of bullying. Cyberbullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue and the age of the learner.

Video conferencing including Zoom

The College only uses approved webcam sites such as Zoom to communicate with other Colleges or for use within lessons. This facility should only be used in agreement with the teacher.

Email

Email is now an essential means of communication which is often accessible by mobile phones. A degree of responsibility must sit with learners, as email access is very difficult to control. Email should not automatically be considered private and emails will be monitored.

Each learner is provided with an email address (@colchester.ac.uk) which is filtered by the College to ensure that learners do not receive unwanted mail. Under no circumstances should learners sign up or sign others up to SPAM. Emails are visible to the ILT team if required.

Emails should not be sent that would be considered as bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or affects the reputation of an individual in the College or the College itself.

If you consider that any e-mail you receive is offensive, likely to contain a virus or chain-mail, do not respond to it and report it immediately to your teacher/tutor who will inform the ILT Director

If any such mail has been generated and received internally, your teacher will report it immediately to the ILT Director, with a forwarded copy if appropriate.

Internet use

The internet in College should primarily be used for College work related to tasks set by your teachers. Personal use (or any other use) of the internet is not permitted during lesson time. You may access the internet for personal use during breaks or during after College activities. Complaints regarding the misuse of the internet will be dealt with by the ILT Director.

Downloading

For the benefit of the whole College community, you may not download, send or email anything:

a) Which may be embarrassing to the College, its learners, staff or governors
b) That is illegal, obscene, sexually explicit, offensive, damaging or which may be reasonably considered by others to cause distress, harassment or discrimination.

Downloading files, shareware or freeware may introduce viruses to the College. In addition, downloading may infringe the terms of the College's licence agreement. Therefore, approval should be sought from the ILT Director.

Educating the Colchester Institute Community

E-safety is not a standalone topic that can be delivered by one department. To be successful it requires all stakeholders to work together.

Further information can be found at;

www.ceop.police.uk

www.thinkuknow.co.uk

www.iwf.org.uk

www.pitda.org