E-Safety & ILT Code of Conduct Policy for Learners

Policy Details			
Policy Owner	Director of ILT		
CE Sponsor	Vice Principal: Curriculum Innovation and Business Transformation		
Date created this year	15 November 2024		
Version:	**Approved by:**	**Date approved:**	**To be reviewed:**
1.1	College Executive	14 February 2025	May 2025

Version Control	
Version Number	**Changes from previous 12 months policy**
1.1	Simplification of Email section
1.1	Small update to Educating the Colchester Institute Community section
1.1	Addition of AI Tools and Usage section
1.1	Internet Filtering – additional wording regarding DfE Cyberbullying section changed to Staying Safe Online and reworded
	Changes to policy in year
2	
2	
2	

Equality Impact Assessment Tool

		Yes/No	Comments
1	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	Race or ethnicity	No	
	Disability	No	
	Gender	No	
	Religion or belief	No	
	Sexual orientation	No	
	Age	No	
	Marriage and Civil Partnership	No	
	Maternity and Pregnancy	No	
	Gender Reassignment	No	
2	**Is there any evidence that some groups are affected differently?**	No	
3	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4	**Is the impact of the policy/guidance likely to be negative?**	No	
5	**If so, can the impact be avoided?**	N/A	
6	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7	**Can we reduce the impact by taking different action?**	N/A	

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

Introduction

Information and Learning Technologies (ILT) enable almost everything that we do in College, whatever our role. It is integral to= 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 ILT including computers, wifi, the internet, mobile devices and technological tools that are designed to hold, share, process or receive information. . 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

- Online Safety Acceptable Use Agreement for Students
- Dealing with Bullying, Harassment and Sexual Harassment at College

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, and the College policies hubon Sharepoint.)
- Policy to be part of College induction pack for new learners
- 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 year 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 computer systems including the 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, Moodle and other platforms 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 oruser errorin 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, chromebooks, tablets, collaboration tools, internet technologies (including AI and search engines), 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. Personal devices should not be used to record, take, or share images, video, or audio without the explicit consent of those involved. 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. Any Bullying and Harassment via any personal device will be addressed in accordance with the relevant College policies.

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 the ILT Department, 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 where appropriate 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.

The College complies with the Department for Education (Keeping Children Safe in Education) standards for filtering and monitoring. The standards include:

- identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet safeguarding needs.

The College's Designated Safeguarding Lead and Deputy Safeguarding Lead work together with the ILT department on filtering and monitoring to ensure a joined up approach.

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 advised 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 oversees security of the user's data but users are responsiblefor 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 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.

Staying Safe Online

With young people spending a considerable amount of leisure time online and Colleges utilising the online space to support learning, it is essential that we work together with learners and apprentices, parents/carers, and external agencies to safeguard young people from potentially harmful and inappropriate online material.

The College recognise that learners and apprentices live in an increasingly complex world, living their lives on and offline. This presents many positive and exciting opportunities, but we recognise it also presents challenges and risks.

Any learner or apprentice can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage, and personal circumstance.

The range of online risks could be categorised as:

content: being exposed to illegal, inappropriate, or harmful material; for example, pornography, fake news, suicide, racist or radical and extremist views

contact: being subjected to harmful online interaction with other users; for example, peer to peer pressure, commercial advertising as well as adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, or online bullying

commerce: risks such as online gambling, inappropriate advertising, phishing and / or financial scams

The College have systems in place to filter and block internet access to harmful sites and inappropriate content. These systems are monitored and regularly reviewed to ensure that they are effective. Staff have all undertaken online safety training and are aware of their role within online safety and monitoring. Staff are aware that any concerns about online safety must be reported to the Safeguarding team.

The College raises awareness and teaches learners about online safety in the following ways:

- For Study Programme Leaners – via the Personal Development sessions
- For Adult learners – via the You Matter Platform
- For Apprentices – via the Assessors, coaches and You Matter Platform

Video conferencing (e.g. Teams and Zoom)

The College only uses approved software such as Teams to communicate with other Colleges or for use within lessons. This facility should only be used in agreement with the tutor.

Email

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 phishing content, 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 provided at the 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.

AI Tools & Usage

The College recognises the potential of Artificial Intelligence (AI) tools to support learning. However, it is essential that learners use AI responsibly and in a manner that aligns with the College’s academic and ethical standards.

Learners are prohibited from sharing personal or sensitive data with AI tools, especially if the tool is not provided or approved by the College. The College is not responsible for any data breaches or privacy risks resulting from the use of unauthorised AI tools. Learners must avoid using AI to generate inappropriate, offensive, or harmful content. AI-generated content should adhere to the same ethical and behavioural standards expected in all College work. Learners must not use AI to complete assignments or exams unless explicitly permitted by their teacher. Misuse of AI in this context will be treated as academic misconduct.

Educating the Colchester Institute Community

E-safety requires collaboration across departments, with ILT and Student Services working together. Resources like CEOP, ThinkUKnow, and NSPCC are available to support further education on e-safety and digital citizenship.

Further information can be found at;

www.ceop.police.uk

www.thinkuknow.co.uk

www.iwf.org.uk

www.pitda.org