Colchester Institute

IT Code of Conduct

Staff, visitors and contractors

This document is prepared and managed by IT Services on behalf of Colchester Institute and is intended for users and system administrators and relates to the IT security standards maintained across all IT systems within the College.

Document Controls:

Document Name: - IT Code of Conduct (staff, visitors and contractors)

	Name:	Title:	Date:
Owner(s):	Chris Adams	ILT Director	31 August 2018

Revised by	Date	Changes	Approved	Version
Chris Adams, ILT DIR	31 August 2018	Reworked from *"Code of practice for the use of IT April 2015"*	CE 31 August 2018	v1.0
Next review date : August 2019				

Information Security and e-Safety

The College is committed to ensuring the integrity of computer based information required for its operation and compliance with relevant legislation as detailed below. To maintain this integrity in what can be regarded a transient medium, the College believes that it is essential to establish and conform to clearly defined standards of operation in relation to computer based information.

The College also wishes to protect all users and students using e-technology either on College IT Systems, PCs, Laptops, remotely or when accessing the internet via their own devices (via College Wifi) and to minimise risks and deal with any infringements.

The College aims to make users aware of this code of conduct during staff induction and from time to time in staff training sessions as required. It should be read in conjunction with the IT Security Policy which is available on the College's IT portal pages.

Principles of Implementation - Scope

The ILT Code of conduct covers all internal College systems and connections to wider networks and is applicable to all users other than students who are subject to their own Code of conduct. It is the responsibility of all such users to comply with this code of conduct. Failure to comply could result in disciplinary procedures being invoked.

Legal Consequences of Misuse of facilities

In a growing number of cases involving the civil or criminal law, email messages (deleted or otherwise) and internet history files are produced as evidence in a permanent written form. There are number of areas of law which apply to use of email and internet and which could involve liability of users or the College.

These include the following:

Intellectual property: Anyone who uses email to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them.

Obscenity: a criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.

Defamation: as a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email and may lead to substantial financial penalties being imposed.

Data Protection: processing information (including photographs) which contains personal data about individuals requires the express written consent of those individuals. Any use of personal data beyond that registered with the Data Protection Commissioner will be illegal. Users who input data on to the College's networks and systems are responsible for ensuring that they comply with the requirements of Data Protection Law. This is encapsulated in the Colleges Data Protection Policy and Retention of Records Policy. Other legislation to consider:

- Computer Misuse Act 1990 Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003

- Terrorism Act 2006 s3
- Police and Justice Act s35-38

Discrimination: any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995 where it involves discrimination on the grounds of sex, race or disability.

Copyright: the use of copyright material where permission has not been gained from the Internet is forbidden as is downloading and file sharing from certain sites. If in doubt check before you use it.

Radicalisation Procedures and Monitoring: Under the Prevent Duty 2015 the College has a statutory duty to “Prevent” staff and students from being radicalised. It is important for us to be constantly vigilant. Staff are reminded to refer any concerns relating to radicalisation and/or extremism (online or otherwise) through the appropriate channels (via The Safeguarding Procedures to Safeguarding Officers). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and students.

E-Safety and Safeguarding

Colchester Institute has a duty of care to Safeguard students from harm and abuse. Students must also take responsibility to safeguard themselves when online. In regard to e-safety this includes safeguarding from online:

- Grooming
- Bullying and or Harassment
- Trolling
- Radicalisation
- Phishing
- Exploitation (sexual, financial)
- Bribery
- Keeping personal information personal
-

The College will provide opportunity for students to explore keeping themselves safe online during and group tutorial sessions.

Monitoring e-Safety, complaints and concerns

The College asks all students and staff not to access, to be vigilant of others and report all concerns to senior management about any student or staff member accessing, loading, sharing and/or sending any content and/or materials deemed offensive, unpleasant, obscene or of a criminal nature. This could include (but not limited to) sexual content; hate crime; extremist content.

Using the Internet

Reasonable private use of the internet is permitted within non-working time but should be kept to a minimum. The Use of the College Internet Connection to download or distribute copyright material is strictly prohibited.

All website use is logged and activities can be monitored. The log records the name of the login user, the IP address of the computer used, the time and date and the address of the website. The log also contains the amount of time spent on the web and also the type of site as categorised by the filtering system i.e. Social, Media, Education, News, Gambling, Business, Entertainment etc.

Sites deemed as unacceptable by the College cannot be accessed via the network. A web filtering system is in place that denies access to such sites. Misuse identified by the filtering system will be reported to a senior manager, and disciplinary action may be taken.

Any user who feels they have accessed an inappropriate site should notify either the IT Service Desk (it.servicedesk@colchester.ac.uk) or the Web Filtering (web.filtering@colchester.ac.uk) with the subject header **ATTN: WEBSITE TO BE CHECKED**. The web site address should then be copied into the email and the site then exited.

Using Email

Emails should be drafted with care. Due to the informal nature of email, it is easy to forget that it is a permanent form of written communication and that material can be recovered when it is deleted. It is admissible evidence in a court of law.

If you send, copy or forward emails with any libellous, defamatory, offensive, racist or obscene remarks, both you and the College can be held liable.

If you unlawfully send, copy or forward confidential information, both you and the College can be held liable.

Email congestion can be avoided by not sending trivial messages or unnecessarily copying emails. Employees should regularly delete unnecessary emails to prevent over-burdening the system.

Reasonable private email is permitted but should not interfere with your work. The content of personal emails must comply with the restrictions set out in these guidelines.

By sending emails on the College’s system, you are consenting to the processing of any personal data contained in that email. If you do not wish the College to process such data you should communicate it by other means.

Due to the unsecured nature of e-mail, alternative methods of communication should be considered if you have to send personal / sensitive data. If you need to send this type of data by email you should password-protect the file and send via email and then send a separate email with the password. Please refer to the data protection policy before sending any information of this nature.

In some circumstances it will be necessary to access some/all electronic files and the email account of a former member of staff, e.g. to gain access to work related information that the user has stored under their IT account and not copied to their manager/team/colleagues prior to leaving.

When an employee is leaving, HR will email the IT Services department who will send out an email to the member of staff copied to their line manager asking them to clear their IT account of personal material/ emails so that only business items remain on the account..

Information is normally archived for six months following the end of employment and then removed from the system, if an individual is aware that business information they hold on their account will be required by the College at a future date they should inform their line manager. A request must be made by CMG/CE to get access to archived accounts of staff that have left.

Access to a staff member’s Colchester Institute IT account or Colchester Institute email system will be made available to the staff member’s line management, Human Resources or IT personnel, where there is good reason to do so, for example due to staff absence or to facilitate an investigation.

Electronic Storage

College systems should be used to store data and information relevant to college operations. Relevant information should be retained in line with the College’s data retention policy, and any data that exceeds stated retention policy should be immediately deleted. Duplication of files should be avoided. Staff should not use college systems for storing personal information.