utc cambridge
Delivering Future Scientists

University Technical Colleges®

UTC Cambridge
ICT Policy

Lead member of SLT: HR/Business Manager
Designated Governor: Safeguarding lead

Associated documentation
UTC Cambridge Equality and Diversity policy
UTC Cambridge Disciplinary and appeals policy

UTC Cambridge Vision
UTC Cambridge: Delivering Future Scientists

UTC Cambridge Mission
Through an innovative curriculum, developed with leading scientists from industry and academia, UTC Cambridge builds bespoke learning solutions delivered in a state of the art science and technology environment that empowers students to manage their academic and career development.

UTC Cambridge Values
We set ourselves challenging goals, are agile and resilient, to achieve our personal best.
By respecting one another we enhance our experience and benefit from different perspectives.
We take individual responsibility, ensuring team delivery.
By respecting our environment, our world, we make a difference.
We celebrate positive contribution and aspire to excellence.
We are morally and ethically responsible in scientific and environmental innovation.

Contents

Review date: July 2017

1. Introduction

1.1 This document outlines the Policy in force at University Technical College Cambridge (UTC) relating to the Internet & College Networks and Compliance of software licencing.

2. Scope

2.1 This policy statement refers to all members of the UTC (staff, students, contractors, visitors) accessing all types of on-line services through University Technical College Cambridge's IT Services.

2.2 Computer hardware or equipment refers to that owned by or connected to the UTC networks irrespective as to its location. This includes microcomputers, networks, personal computers, laptops, workstations, minicomputers, tablets, iPads, mobile phones, Smartphones, personal digital assistant (PDA) and multi-user systems, collectively called computer systems.

2.3 The University Technical College Cambridge (UTC) IT Manager and the relevant IT Team are the designated authority within the UTC for all matters relating to the use of computer systems.

3. Purpose

3.1 Breach of this policy document will lead to investigation and may lead to disciplinary action against the offender via existing UTC HR disciplinary procedures. The UTC reserves the right to report to the Police any action/activity considered unlawful. Criminal proceedings may follow as a result.

3.2 The UTC systems are to be used for the academic and administration purposes of the UTC. They must not be used inappropriately; where accesses to normally inappropriate resources are required it is so only for genuine curriculum reasons and after approval is sought from Principal or their delegated authority.

3.3 The IT Support Team are responsible for the provision of user accounts and passwords, no attempt should be made to access systems without obtaining prior authorisation to do so.

3.4 Commercial or distribution activities are prohibited on UTC Systems unless formally sanctioned by Principal or their delegated authority.

3.5 Activities likely to damage the reputation of University Technical College Cambridge are prohibited.

3.6 All users are responsible for understanding and following the Cambridgeshire County Council computer services acceptable use policy. Queries with regards to the acceptable use should be forwarded to the IT Support Team via email or directed to the Helpdesk on 01223 724360

4. Monitoring of College Systems

4.1 The Principal or their delegated authority, ISP or ISP Cert may order the monitoring or interception of system logs, web pages, email messages, network account or any other data on any computer system owned by the UTC for the following reasons:

To prevent or detect crime
To ascertain compliance with regulatory standards
To monitor communications in order to establish whether they are business related
To investigate or detect unauthorised use of telecommunication systems
To secure the systems

All such monitoring processes will be performed in accordance with the Data Protection Act, the Regulation of Investigatory Powers Act (RIPA), the Lawful Business Regulations (under RIPA) and Human Rights Act.

The IT Support Team reserves the right to inspect and validate any items of UTC owned computer equipment or any equipment connected to UTC Networks.

Any computer equipment can be removed by IT Support team if it is deemed to be interfering with the operation of the network.

For security and legal reasons the UTC may record and keep audit data generated when users access systems at the College.

The UTC Cambridge is legally obliged to report to the police the discovery of certain types of electronic data, if it is found on the College equipment or transmitted across the Colleges networks.

5. Prohibitions – Internet/Networking

5.1 The creation, storage, transmission or viewing (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

5.2 The creation of any links to external, offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

5.3 The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety, or which brings the UTC into disrepute.

5.4 The creation of transmission of defamatory material.

5.5 The transmission of material such that this infringes the copyright of another person.

5.6 The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks.

5.7 Deliberate unauthorised access to facilities or services accessible via the UTC Cambridge's Internet connection.

5.8 The unauthorised access of UTC Systems by your negligent actions.

5.9 The dissemination of information which may lead to the unauthorised modification of computer materials (modifications would include activities such as the circulation of "infected" software or the unauthorised use of a password).

5.10 The changing of function or role of any system or networking component within the College's network without the permission of IT Support Team.

5.11 The setting up of any network service (web services, email servers etc) without the prior permission of IT Support Team. This includes web shares and music/MP3 sharing peer to peer applications such as BitTorrent and those which abuse the available bandwidth of the organisation such as Movie Streaming sites.

5.12 The amending or deleting of data structures of other users without their prior consent.

5.13 The introduction either wittingly (or through negligence) of harmful or nuisance programmes, files, worms or spyware onto any computer system which is likely to prevent its full use or cause damage to any of the UTC systems or services.

5.14 The registering of any domain name which includes the name of the University Technical College Cambridge or any name (including email addresses) which would mislead the public into believing the name refers to University Technical College Cambridge or the staff/student there in.

5.15 The placement of links to sites which facilitates illegal or improper use, access to copyright files, unlawful distribution or display of pornographic material.

5.16 Staff are forbidden from using the internet to enter financial or contractual agreements on behalf of the organisation including on-line subscriptions unless they are authorised to do so and made within the framework of the UTC financial regulations and approval of the Principal or their delegated authority.

5.17 Deliberate activities with any of the following characteristics:

Corrupting or destroying other users' data.
The use of or downloading of tools which could be used to gain access to protected or restricted parts of the UTC or a partner institution's computer systems.
Any act described by the term "hacking".
Violating the privacy of other users.
Disrupting the work of other users.
Using the College's Internet connection in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment).
Other misuse of any networked resources, such as the introduction of "viruses, Trojans or spyware".

5.18 Where the UTC Internet connection is being used to access another network, any abuse of the acceptable policy of that network will be regarded as unacceptable use of the UTC networks.

6. Security

6.1 It is unacceptable to provide anyone with your username and password. You must not reveal your passwords to anyone. All passwords should be created to provide maximum protection (the use of the word 'password' as an entry is unacceptable and would constitute misuse). System passwords should be changed every month. Passwords should incorporate both letters and numbers and should be at least 8 characters in length. Further guidance on good practice with regards to passwords can be obtained from the IT Support team.

Passwords can be changed by users when logged into the network by pressing CTRL+ALT+DEL and selecting Change a Password… or at the IT Support Helpdesk.

6.2 You must not violate the privacy of others on the computer systems.

6.3 For your own security you must not leave your workstation logged-in when unattended, to lock a workstation press CTRL+ALT+DEL keys together, or contact IT Support on 01223 724360 for further guidance. Any damage caused due to negligence will be initially directed at the account holder.

7. Email

7.1 You must not send unwanted email (Spam).

7.2 You must not post or send binary files to email groups or other areas such as USENET groups.

7.3 You must not create or transmit chain letters, hoax virus warnings, pyramid letters or similar schemes using email.

7.4 You may not send rude or inflammatory emails to other users

7.5 The UTC email accounts are owned by University Technical College Cambridge. The accessing of other mailboxes is strictly prohibited unless authorised in writing by the mailbox owner or contact IT Support on 01223 724360 who will attempt to gain approval Principal or their delegated authority and Human Resources. Access will only permitted in exceptional circumstances; users should ensure a localised policy is in place for covering leave and long term sickness.

7.6 Users should ensure email accounts are checked at regular intervals, a minimum is once a day, any accounts found to have fallen into a dormant state for more that 5 weeks will be disabled.

7.7 Messages stored in inbox (and any sub folders), deleted items and sent items should be purged at regular intervals, a maximum timescale for retention is one month. Those emails required for longer storage should be transferred to Personal Folder files, details of how to achieve this can be obtained from the IT Support Team.

7.7 The use of Folders is encouraged, as this will provide better management of the inbox, further information on creation of the folders can be obtained from the Communication Systems team.

7.8 Large attachments should not be included on emails unless the sender is aware that the recipient could easily open the attachment or receives authorisation from the IT Support team. It should be noted the system has measures in place to restrict attachment size to a maximum of 20Mb.

7.9 The UTC has a number of measures in place to restrict spam, however spam will still arrive, it is expected users will undertake reasonable care when accessing email attachments, and if unsure contact should be made with IT Support team before opening something attached to a email.

7.10 External links should never be followed from external emails, as these may be malformed addresses which can lead to infection of systems with malware.

8. Software Licensing

8.1 All computer software acquired by University Technical College Cambridge must be purchased through the IT Support Team. No user may purchase software and the purchase of software by any other means such as UTC Purchasing Cards/Credit Cards, expense accounts or petty cash is expressly forbidden.

8.2 All newly purchased software will be delivered to the IT Support team so that licences can be checked and Asset Registers updated. No other staff may take delivery of computer software.

8.3 Computer Software can only be installed by the IT Support Team under no circumstances is computer software be installed by any other member of University Technical College Cambridge staff.

8.4 All staff or department moves must involve the IT Support team so that the appropriate software can be added or removed and asset registers updated.

8.5 The Disposal of Software/Hardware used by University Technical College Cambridge may only be carried out by or under the direct supervision of the IT Support Team.

8.6 Shareware, Freeware & Public Domain software is bound by the same policies and procedures as all software. No user may install any free or evaluation software onto University Technical College Cambridge systems.

8.7 The UTC Cambridge will not tolerate the use of any games, music downloads, font files or screensavers other than the company standard screensaver, or the games, fonts which form part of your operating system.

8.8 The UTC Cambridge software policies apply to mobile users and all laptops will be equipped with UTC Cambridge auditing software for regular checks.

8.9 All users must be aware that the UTC electronically audits all computers on a monthly basis. Sample random audits may be carried out without notice. The UTC IT Support team reserves the right to inspect portable devices and media to ensure compliance of the encryption of data in line with the College Data Protection policy.

9. User Responsibility

9.1 Backups are carried out on the mission critical servers for disaster recovery purposes only; users should ensure that files stored on these servers are backed up locally at regular intervals, along with any files stored on other mediums. Many applications such as those within Microsoft Office have the facility to auto-save, it is recommended that users adopt best practice and activate these.

9.2 Where possible users should ensure that all correspondence is Spell Checked to ensure a high image of the UTC is projected to all recipients. Users are urged to use the automatic spell checking facilities incorporated in a number of applications.

9.3 Violations in the use of the Internet, Networks or Email should be reported to the Head of Communications & IT, by telephone 01223 724360 (ext. 4360) or email abuse@utccambridge.co.uk all complaints will be investigated fully and findings where appropriate will be reported back to the plaintiff.

9.4 Information important to UTC Cambridge received by email or other medium should be securely stored, if necessary as a hard copy, in addition comments made via email should be based on facts alone.

9.5 No users of UTC Cambridge Systems (desktops, laptops, PDA's, Tablets, Mobile Phones etc) are allowed to install any software. This includes software downloaded from the internet e.g. freeware/shareware. All software installations are to be carried out by the IT Support Team on 01223 724360. It must be noted that all instances of non compliance will be taken forward for formal investigation. (See 10.1).

9.6 UTC Policy is that Data should not be removed from site unless deemed necessary, and should be accessed only via a secure VPN Connection after agreeing to the Terms and Conditions of VPN Use – available from the IT Support Team.

9.7 To maintain Data Protection staff are required to encrypt sensitive college data while transporting off college networks using only UTC owned USB Memory Sticks, External Hard Drives, Laptops, Portal devices and College approved internet based services/The Cloud. Free encryption software is available at www.truecrypt.org/ – further Advice and guidance on encryption methods are available from the IT Support Team. Sensitive data should never be transported un-encrypted – and even when encrypted should be retained for only the length of time necessary.

9.8 Portable devices carrying sensitive information should always be passed to the IT Support team for secure disposal.

9.9 Sensitive and confidential information should never be emailed outside the organisation un-encrypted.

9.10 Staff should read and comply with all measures detailed in UTC E-Safety guidance and policy. The IT Support Team reserves the right to carry out spot checks of UTC owned Portable

Storage devices and Mobile computing/Tablets and Mobile Phones to ensure the compliance of College Data protection policies.

10. Liability & Related Matters

10.1 The UTC Cambridge will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of any IT facility provided. The UTC Cambridge takes reasonable care to prevent corruption of information and strives to maintain
effective security on all of its computer systems. However, it cannot and does not give warranties about the integrity of information or about the security or confidentiality of data (including electronic mail) or other materials submitted or processed by the UTC Cambridge. It may be necessary on occasions for selected UTC staff to gain access to password protection information stored on the computer systems.

10.2 Neither the UTC Cambridge nor any of the UTC employees or associated or delegated entities will be held responsible for the correctness or otherwise of results produced by using its computer facilities.

10.3 While every reasonable endeavour is made to ensure that the computer systems are available as scheduled and function correctly, no liability whatsoever can be accepted by the UTC for any loss or delay because of equipment malfunction.

10.4 If as a result of misuse of the computer systems an individual causes the UTC Cambridge to be involved in legal action, the UTC Cambridge reserves the right to take consequential action to recover losses.

11. Disciplinary Action

11.1 Breach of this policy document will lead to investigation and may lead to disciplinary action against the offender via existing disciplinary procedures. The University Technical College Cambridge reserves the right to report to the Police, any action/activity considered unlawful. Criminal proceedings may follow as a result.

12. Enquiries and Change Control

12.1 All enquiries relating to the content of this document should be directed to the Author.

12.2 This document will be subject to a yearly review. The review will be initiated by the IT Manager.

12.3 Any changes to this document must be agreed by Principal and or their delegated authority.

Appendix1

IT Policy Signature Page

*Please sign and return this document with your enrolment forms. Student account information will not be issued without returned signed document.

I _____ (student) promise to agree and uphold to the rules in this document. I understand that if I am found in violation of any of the rules in this document, it may lead to disciplinary action ranging from wifi/internet ban for minor to complete account disabled or exclusion for major offenses. I understand that destruction of school property, including IT equipment, will result in sanctions up to and including financial restitution. I also understand that The University Technical College Cambridge reserves the right to report to the Police, any action/activity considered unlawful. Criminal proceedings may follow as a result.

Student Name (Print): _____

Student Name (Signature): _____

Parent Name (Print): _____

Parent Name (Signature): _____

Appendix 2. Social Media Guidelines

Please follow the summary list of 'do's' and 'don'ts' for all online communication with Students. If you require further specific advice please contact The Designated Safeguarding Officer.

DO:

Ensure that anything you post online via email/social networking/VLE is in accordance with your relevant General Teaching Council (GTC) code of conduct. Specifically, the eighth principle of the GTC Code of Conduct in England states a teacher must "demonstrate honesty and integrity and uphold public trust and confidence in the teaching profession".

Only use and share your College email address and phone number for communication with Students.

Only use equipment e.g. mobile phones, provided by UTCC to communicate with Students, making sure that Students have given permission for this form of communication to be used and that parents/carers have given written permission for this communication with under 16's. Consent for this type of communication has been added to both the application form and the enrolment form from September 2011.

During UTCC trips always use a UTCC mobile phone to communicate with Students.

Recognise that text messaging is rarely an appropriate response to a young person in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible.

Use the VLE to contact Students and to share information with them appropriately.

UTCC recommends that you inform your line manager about any Student aged under 18, who you might be "friends" with on a social networking site e.g. family member, close friend. This can protect staff should any inappropriate social networking use occur.

Report and log any communication received from Students that you feel may be inappropriate, as soon as possible after the communication. Report this to your line manager, HR or one of the Designated Safeguarding Officers.

DO NOT:

Allow Students access to your own social networking space(s) including Bebo, Facebook, Myspace, Twitter etc. Request from Students to add them to your "friends" list within these sites should NOT be accepted.

Communicate with Students via your personal home email account.

Provide Students with your personal mobile or home phone number, or your home email account.

Lend a Student your personal mobile phone. If a phone is needed supervise the Student using a UTCC mobile or supervise the use of a UTCC phone.

Share any of your personal information with Students. For example, do not share details such as your home address, date of birth, personal mobile or home telephone numbers and financial status with Students to preserve your privacy and maintain professional boundaries at all times.

Request, or respond to, any personal information from a Student other than that which might be appropriate as part of your professional role e.g. you may need a Student's emergency contact details for a trip that you are taking the group on, therefore it is appropriate to ask for this. However it would not

be appropriate if a Student had asked you for your personal mobile number so that they can call you during the weekend (even if the phone call would be related to UTCC). It is best to advise the Student to meet with you during the UTCC day to discuss their query.

Cyberbullying

Staff should never retaliate to cyberbullying incidents in a personal way. Please report incidents to your line manager or Human Resources at the earliest opportunity.

It is important to keep records of the abuse as the bully will leave a 'digital footprint' that can potentially be used as evidence against them e.g. texts, emails, social networking wall feeds, voice mails and instant messages. Do not delete texts or emails. Take screen prints of messages or web pages, and be careful to record the time, date and address of the site.

Where the perpetrator is known to be a Student or member of staff, the majority of cases will be dealt with through the UTCC's Student Behaviour or Staff Disciplinary procedures.

Some cases of cyberbullying may involve a type of identify fraud e.g. "frapping" where someone has gained access to another person's personal email or social networking page, pretends to be that person, and then sends cyberbullying messages. It is important to bear the possibility of this in mind and not to accuse or contact anyone until a full investigation has been carried out.

Where there is evidence that the law has been broken e.g. death threats, assault, hate crime, staff will be advised to contact the police directly after notifying their line manager.

If a potential criminal offence has been committed and UTCC is not able to identify the perpetrator, the police may issue a RIPA (Regulation of Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message.

Support will be offered to the person being bullied throughout the investigation process by their line manager and Human Resources.

In cases where an allegation is made that an employee or volunteer has: behaved in a way that has harmed or may have harmed a child/young person/vulnerable adult; possibly committed a criminal offence against or related to a child/young person/vulnerable adult; or behaved towards a child/young person/vulnerable adult in a way the indicates s/he is unsuitable to work with children/young people/vulnerable adults, then that allegation should be reported to Human Resources immediately. The Local Authority Designated Officer will be contacted and will provide advice and monitoring of this case.

In a teaching environment, if a Student is suspected of taking a photo of a member of staff maliciously, or without consent, the mobile phone can be confiscated and placed in the safe at reception, as a disciplinary penalty. Staff can call security who can assist with any incident of this kind.

Staff may become aware of other people posting objectionable material about them or other staff, through reports from other Students; therefore it is important for all staff to report any incidents they become aware of to Human Resources immediately.

UTCC will advise staff of third party agencies they may contact to request that inappropriate material is removed, where possible. This includes mobile phone providers, social network sites, video and hosting sites, instant messengers, chat rooms, forums and message board hosts. More information and advice about this can be found at www.teachernet.gov.uk/publications ref: DCSF-00242-2009 Cyberbullying Supporting School Staff.

Photographic Images

The following guidelines should be adhered to when taking, posting or displaying photographic images:

When taking photographs of Students, explain to Students the purpose of the activity and what will happen to the images when the activity is concluded.

Ensure the Students understand why the images are being taken and has agreed to the activity and that they are appropriately dressed.

Do not take, post, distribute and/or display images of Students online without their written consent and without parental/carer written consent if under 16 or if the student is a vulnerable adult. A vulnerable adult is a person aged 18 years or over who is or may be in need of community care services by reason of mental or other disability, age or illness; and who is or maybe unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation.

Images that are posted online should only be in the context of enhancing the educational experience and should not have personal information attached to them e.g. full names, dates of birth without informed and/or parental/carer written consent. Even with consent, care should be taken to be mindful of basic e-safety practice.

As a member of staff you should be able to justify the images of Students that you have in your possession.

Avoid making images in one to one situations or which show a single Student with no surrounding context.

Only use equipment provided or authorised by UTCC.

It is your duty to report any concerns about any inappropriate or intrusive photographs found of Students.

Do not use images which may cause distress to Students.

Do not use personal mobile telephones to take images of Students.

Do not take images 'in secret', or take images in situations that may be construed as being secretive.

Ensure that Students of any age are not exposed to unsuitable material on the internet.

Always ensure that any films or material shown to Students are age appropriate and take into account any equality and diversity needs.

Glossary of Terms

WEBSITE

Bebo is a social networking website launched in July 2005. Bebo is very similar to other social networking sites, mainly Facebook.

Facebook is a social networking service and website launched in February 2004. Facebook has more than 600 million active users. Users may create a personal profile, add other users as friends, and exchange messages, including automatic notifications when they update their profile. Facebook users must register before using the site. Additionally, users may join common-interest user groups, organized by workplace, school or college, or other characteristics.

Myspace is a social networking website and is a free online community composed of personal profiles aimed foremostly at a younger membership. A MySpace profile typically includes a digital photo and in-depth information about personal interests. The amount of detail included in the profile is up to the user and submitted voluntarily.

Twitter is a website, owned and operated by Twitter Inc., which offers a social networking and microblogging service, enabling its users to send and read messages called tweets. Twitter has gained

popularity worldwide and is estimated to have 200 million users generating 190 million tweets a day and handling over 1.6 billion search queries per day. It is sometimes described as the SMS of the Internet.

YouTube is a video-sharing website on which users can upload, share and view videos. The company uses Adobe Flash Video and HTML technology to display a wide variety of user-generated video content, including movie clips, TV clips, and music videos, as well as amateur content such as video blogging and short original videos.

LinkedIn is a business-related social networking site mainly used for professional networking. Users maintain a list of contact details of people with whom they have some level of relationship, called connections. This list of connection can then be used to build up a contact network, follow different companies and find jobs, people and business opportunities.

Flickr is an online community in which users share photographs with each other.

Instagram an online photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, apply digital filters to them, and share them on a variety of social networking services, such as Facebook, Twitter, Tumblr and Flickr.

Pinterest is a pin board-style photo-sharing website that allows users to create and manage theme-based image collections such as events, interests, and hobbies. Users can browse other pin boards for images, "re-pin" (share/re-tweet) images to their own pin boards, or "like" photos.

Tumblr is a site which allows users to post multimedia and other content to a short-form blog.

TERM

Tweets are text-based posts of up to 140 characters displayed on the user's Twitter profile page.

Re-tweet is to repost another user's message on Twitter.

Share is to repost another user's message on Facebook.

Blog is a type of website or part of a website usually maintained by an individual with regular entries of commentary and descriptions of evens (blogging). The content of a microblog is simply smaller in size.

Comment is a response that is often provided as an answer or reaction to a blog post or message on a social network. They are available to view by others.

Follow is a term applied to Twitter in which users subscribe to other user's tweets.

Forum is the term used for message board, an online discussion site. It is the modern equivalent of a traditional bulletin board.

Friends is used in the context of Facebook. Friends are those who you give access to your personal profile. Access can be restricted by certain privacy settings.

Connections is used in the context of LinkedIn. Connections are those who you give access to personal profile. Access can be restricted by certain privacy settings.

Hash tag is used on several social networking sites as a way to annotate a message. A word or phrase is proceeded by a '#' e.g. '#goodday'. Hash tags are often used to show that the message is related to an event or to trend (see term below).

Trend is seen on every social network. Facebook shows what is trending e.g. royal baby is born, when multiple users are sharing the same link or discussing the same topic. Hash tags is common method of allowing your message to trend.

Like is an action that is made on Facebook. A user can click the 'like' button to shows their approval and share the message. Depending on privacy settings, other Facebook users may be able to view.

Post is the term used when a user adds a new blog or forum.