

University for the Creative Arts

IT Use Policy

(STUDENT)

Version 1.5 – May 2016

Document History

This document has been updated in summer 2011 to add guidance relating to web 2.0 and cloud technologies. The update in summer 2012 reflects changes following the Academic Management Structure Review. In May 2016 this document was been updated to incorporate new the Counter Terrorism and Security Act and compliance with the Prevent Duty.

Version History

1.0	July 2009	
1.1	September 2010	IT Services
1.2	July 2011	IT Services
1.3	September 2011	IT Services
1.4	August 2012	IT Services
1.5	May 2016	Director of IT Services

1 Introduction

The University for the Creative Arts, (referred to hereafter as “the University”), promotes and facilitates the proper use of Information Technology in the interests of learning, research, creative practices, and business operations.

Because the University is ultimately responsible for the proper use of its IT Facilities, it can therefore be held liable for any abuse of their use which breaches English or European Law, the policies of umbrella organisations, or breaches the contracts the University has with external service providers, such as JANET*.

This policy will refer to all computing tools, systems, services supplied or used, and electronic communications tools, (including telephony), the associated physical environments, and any associated support as ‘UCA IT Resources’.

Guidelines and policies change from time to time; therefore, users are encouraged to refer to on-line versions of this and other University policies which are available via the University’s web site. If you have any query on this policy, please email your query to the IT Service Desk – itservicedesk@ucreative.ac.uk

* JANET: the UK’s Education and Research Network. See www.janet.ac.uk

2 Scope

This Policy applies to:

- Students using either personal or University provided equipment connected locally or remotely to the network of the University.
- All equipment connected (locally or remotely) to UCA IT Resources.
- Use of external networks and services that support the University’s IT provision
- External entities that have an executed contractual agreement with the University
- Information that is recorded on, processed by, or output from UCA IT Resources
- The use of external online/cloud technologies such as wikis, blogs, discussion forums, social networks, collaboration technologies, file hosting services, data storage services and online office suites that are not part of the UCA software portfolio.

This Policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered. In the first instance students should address questions concerning what is acceptable to their course tutor. Where there is any doubt the matter should be raised with IT Services, whose staff will ensure that all such questions are dealt with at the appropriate level within the University.

The University wishes to encourage the use of appropriate cloud technologies and services, and wherever possible staff and students should use the University’s official platforms and services. Users of externally hosted technologies must ensure that this use is compliant with the law and the issues covered by this policy.

3 Core Principles

3.1 Overarching Legislation and Policies

All members of the University are subject to the Regulations of the University and to English and International law. The use of UCA IT Resources to create, store or distribute material that contravenes these regulations and laws can result in disciplinary or legal actions being taken against both the individuals responsible and the University as an organisation. The University has published specific policies on Information Security and Information Handling which govern much of what is stated in this Policy and users should make themselves familiar with these policies particularly if their usage exposes them to personal or University sensitive information.

3.2 Liability

All users of UCA IT Resources are ultimately liable for what they produce and what they distribute through their use. The University may be equally culpable if it does not have in place policies and procedures to govern and police the proper usage of these facilities.

3.3 Interpretation

The laws that apply to the interpretation and impact of material created or distributed by one person to another are that it is the impact upon the recipient, intended or otherwise, rather than the intention of the creator or sender that applies in cases of harassment or offence.

3.4 Security

All IT systems and the files and media created through their use are valuable University assets that can be easily damaged or lost. It is the responsibility of all users to be aware of these risks and to use these facilities carefully and responsibly.

3.5 Privacy

Neither the IT Services staff and systems administrators nor any other members of the University will inspect individual user emails or content of personal files unless the conditions of the Regulation of Investigatory Powers Act 2000 are met.

4 Acceptance of this Policy

The registration of a student to use UCA IT Resources implies, and is conditional upon, acceptance of this Policy, for which a signature of acceptance may be required on joining the University.

The lack of a signature does not exempt an individual from any obligation under this Policy. It is the responsibility of all users of UCA IT Resources to read and understand this Policy.

5 Ownership and Intellectual Property Rights

Electronic communications documents pertaining to the business of the University are considered University documents whether or not the University owns the electronic communications facilities, systems or services used to create, store, or distribute them.

Electronic files that are created during academic and creative activities, such as, digital images, digital time based media and creative writing remain the ownership of their authors.

When a student leaves the University, files which are left behind on any computer system owned by the University, including electronic email files, will be considered to be the property of the University. It is up to the leaver to ensure that they have cleared their electronic folders of private material.

Before using externally hosted services, users are responsible for consulting the service's terms and conditions to identify any IPR policy that may conflict with the University's IPR regulations. Web 2.0 technology organisers must remind users of the University's IPR regulations prior to use of the technology and of their obligations in relation to the clearance of IPR-protected material.

Due to the risks of confidential information being released into the public domain inadvertently, e.g. information that relates to a potential patent application or is otherwise commercially valuable, UCA does not permit the use of cloud technologies for research collaboration, unless the prior written permission of the relevant research person has been obtained.

Authentic and reliable copies of teaching and learning materials and assessed work that is not hosted on UCA servers need to be managed and retained in accordance with the University's Records Retention Policy.

In the fields of research and administration, cloud technologies must only be used with the prior written permission of the Executive Dean of Learning, Teaching and Research.

5.1 Publishing Externally

Due to reasons of ownership, data protection, intellectual property and copyright, the following content must not be made available on any part of the Internet not hosted by UCA or transmitted electronically without prior authorisation:

- Course handbooks
- Programme specifications
- Unit handbooks
- Essay and dissertation assignments
- Summative feedback or confidential feedback
- Formative assessment feedback
- Staff or student personal information
- Student contact details
- Any media for which you do not have permission to use
- Any material that could be considered defamatory, slanderous or libellous.

5.2 Freedom of Information

Users need to consider whether the use of an externally hosted service or technology will hinder compliance with the duties imposed on the University under the [Freedom of Information Act 2000](#). The cloud is not an appropriate medium for sharing confidential information, and users are responsible for ensuring that information that is exempt from disclosure under the Freedom of Information Act is not posted onto an externally hosted service.

6 Data Protection

Users need to consider whether the use of an externally hosted service or technology will hinder compliance with the duties imposed on the University under the [Data Protection Act 1998](#). Users are responsible for ensuring that all personal information is processed in accordance with the University's Data Protection Policy. The Cloud is not an appropriate medium for sharing confidential information or personal data.

7 Counter Terrorism and Security Act 2015 and the Prevent Duty

Section 26 of the Counter Terrorism and Security Act places a duty on the University to have, in the exercise of its functions, due regard to the need to prevent staff and students being drawn into Terrorism. Under the guidance from HM Government, the University will maintain a record of network activity relating to access, attempted access, web traffic and threat analysis via remote analysis applications and shall take action where required. Data analysis of this nature is essential to ensure that the Security and Compliance of the University's IT infrastructure is maintained by preventing threats and violations including intrusion, unauthorised access, malicious code, licensing, pirating and copyright violations.

It is recognised that there may be instances where students will need to access material which supports terrorism as part of their research activities. Students who wish to access such material will need to receive approval from an academic member of staff and then register their need to access such material with the IT Security and Compliance Manager.

In the event that the University receives an internal or external enquiry regarding suspect security-sensitive material associated with the university or a university member, IT Services should be engaged to ensure that this matter is recorded and where necessary escalates this matter within the designated University's leadership team channels.

8 Purpose of Use

The UCA IT Resources are provided for the use of students to support their academic and creative endeavours. The use of these facilities for personal use, such as personal electronic mail or recreational use of the World Wide Web is a privilege, not a right, that can be withdrawn. Any such use must not interfere with any other person's use of UCA IT Resources and must not, in any way, bring the University into disrepute.

The use of UCA IT Resources in support of non-University related activities requires explicit permission from the Executive Dean. Such use, whether or not authorised, may be liable to charge.

9 UCA & Ucreative Domain

The University uses the registered name UCA and ucreative as its internet domain name and its internet address is www.ucreative.ac.uk. All emails that originate from within the UCA or ucreative domain will incorporate UCA or ucreative in the email address, but this does not mean that the University automatically sanctions the content or views of all emails that originate or are forwarded from its domain. 'UCA' or 'Ucreative' must not be used implicitly or explicitly in any way that suggests the University's endorsement of the content of an electronic data communication where this is not the case. The use of the UCA or ucreative email account is mandatory and must be used for all university email communications. Exceptions to this will be when there is a disaster recovery situation and the email domains are unavailable.

10 Authorisation

The registration procedure grants authorisation to use the core IT facilities of the University. Following registration, a username, password and e-mail address will be allocated. Authorisation to use other services may be granted automatically at the time of registration according to the user's needs, or may be requested at a later date by applying to IT Services or the appropriate systems' administrator.

All individually allocated usernames, passwords, e-mail addresses, and electronic certificates are for the exclusive use of the individual to whom they are allocated.

Users are personally responsible and accountable for all activities carried out under their allocated username.

Attempts to access or use any username, e-mail address or certificate, which is not authorised to the user, are prohibited.

Users must take all reasonable precautions to protect University resources and their personal account details, usernames, and passwords.

11 Passwords

The passwords used to log in to accounts and applications are subject to periodic change, currently set at 90 days. Passwords, once expired, cannot be used again i.e. it is not possible to rotate cyclically through a small set of favourite passwords.

Whenever a temporary password is allocated to facilitate a user's very first access to an account or application, this must be changed immediately following a successful login.

Passwords must not be disclosed to anyone even if the recipient is a member of IT Services support staff.

If you forget your password, contact a Library Technician who will be able to help you.

12 Privacy

No member of University staff, including IT Services' technicians, will inspect individual user emails or content of personal files unless the conditions of overarching legislation in such areas is adhered to (see the University's Information Security Policy). However, there are times when the University is obliged to investigate the material it holds on its systems e.g:

- To ensure the system's security and effective operation: e.g. a virus or large scale blanket e-mail threatens the functioning of the entire system or is likely to delete or corrupt user data.
- To prevent or detect serious abuse of its system usage, crime, or the infringement of IT related legislation such as the Computer Misuse Act 1990.
- Receipt of a formal request from a law enforcement agency to release files that they require in pursuance of investigations that they may be carrying out.

So although the University sees privacy as desirable, it is not an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by authorised members of staff who may have privileged access to such areas to perform investigate duties.

12.1 Systems' Administration and Privacy

Systems administrators and technical staff may be obliged to access any file, including electronic mail, stored on any system for which they have a responsibility to support. As the content of files cannot always be identified through their filename, this may necessitate opening multiple files until the required file or files are located.

Staff engaged in system support activities are bound by confidentiality clauses not to disclose any private information that they become privy to during the course of such activities.

12.2 Network Monitoring and Traffic Intercepts

Regular network monitoring is essential for ensuring that the University's IT systems' function effectively, and any indication that there is a potential risk to its use may necessitate more focussed monitoring of specific network usage and high volume users.

In some circumstances it may be necessary to intercept network traffic in order to specifically identify the cause of performance issues or network bottlenecks. In such circumstances all reasonable steps will be taken to ensure the privacy of users.

12.3 Privacy to Others

When approaching or sitting near a user at a terminal, what they may be working on may be private or University confidential and this privacy must be respected.

Where users share a printer, care must be taken when removing printed output that others printed matter is not retrieved, and if done so in error, the material must be passed to the owner if they are in the immediate vicinity, or left at the printer for them to collect. Users must avoid the temptation to read printed matter that they happen across at a shared printer. Equally, if printing out confidential material using a shared printer, the printed output should be retrieved immediately.

12.4 Use of External Technologies

Users of these technologies must ensure that the University can still access the information locally and that the data is retired in line with the Information Handling Policy. Compliance with the FOI must always be considered in the use of these technologies.

13 Behaviour

No person shall perform any act that could jeopardise the integrity, performance or reliability of IT equipment, software, data and other stored information.

13.1 Connection of Personal Devices to the Network

Although the University has in place sophisticated systems for the prevention of damage caused by the distribution of malicious software (malware), such as computer virus programs, it is the responsibility of users to ensure that any personal device, for which *they* have responsibility and which is attached to the University network, is adequately protected through the use of up to date anti-virus software and has the latest tested security patches installed. See the University policy 'Mobile Working and Remote Access Policy' for further guidance.

13.2 Use of Plug-in Speakers and Headphones

Plug-in speakers must not be used with UCA IT equipment in shared environments such as the Library and Learning Centres and shared office space.

Headphones may be used but only at a volume where there is no sound leakage that could disturb other users. If inconsiderate use of headphones causes a nuisance to other users, such users have a right to ask for the volume to be reduced or else register a complaint with the appropriate authority responsible for managing the shared space in question.

13.3 Harassment and Bullying

Distributing material which is deemed offensive, obscene or abusive, may not only be illegal but may also contravene University codes on harassment. Users of UCA IT Resources must familiarise themselves and comply with the University's code of conduct on harassment and bullying.

13.4 Equal Opportunities and Accessibility

The University, as expressed in its Equal Opportunities' Policy and Accessibility Policy, is committed to achieving an educational and working environment which provides equality of

opportunity, and freedom from discrimination on the grounds of race, religion, sex, class, sexual orientation, age, disability or special need.

14 Unacceptable Usage

14.1 Creative Practice vs Moral and Social Sensitivities

Conventional norms of behaviour apply to IT-based media, just as they would apply to more traditional media, but a policy such as this cannot anticipate all the issues that might arise in the use of IT facilities in pursuance of academic or creative activities, particularly those that border the boundaries of sensitivity regarding religious or moral values.

Where academic endeavours appear to confront such areas, students must liaise with their tutors to ensure that the study or practise is executed whilst recognising the intertwining legal, institutional, individual, and creative interests involved. Within the University setting this should be taken to mean that the tradition of academic and creative freedoms will always be respected and where the integrity of such endeavours can be clearly argued for or demonstrated, the University will seek to support this in a managed way.

14.2 Offensive, Obscene, or Indecent Material

Users must not create, propagate, or retain material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law, (see above).

The creation, dissemination, storage and display of indecent images of children is prohibited.

14.3 Processing Material that Supports Criminal or Terrorist Activities

Users must not create, propagate, or retain material that is associated with the support of terrorism or any other criminal activities.

14.4 Piracy and Intellectual Property Rights Infringement

Any activities which do not conform to UK and International law regarding the protection of intellectual property and data are prohibited. In accordance with the laws relating to Intellectual Property Rights, the downloading and copying of such files without the permission of the owner of the copyright is an illegal practice. The downloading, distribution, or storage of software, music, digital images, video and film clips, or other material for which you do not hold a valid licence, or other valid permission from the copyright holder, is not allowed.

Plagiarism, i.e. the intentional use of other people's material without attribution, is not allowed.

14.5 Abuse and Annoyance

Users must not use UCA IT Resources to harass, bully, or cause annoyance, inconvenience or needless anxiety to others. The creation, dissemination, storage and display of hate literature is prohibited.

The posting of defamatory comments about staff or fellow students on virtual learning environment or social networking sites is not allowed.

14.6 Defamation

Although genuine scholarly criticism is permitted, users must not create, propagate, or retain material that may be defamatory to another person, group, or organisation.

14.7 Email Misuse via Mass Emailing

The use of email for the distribution of emails to multiple addresses via email groups for frivolous or promotional purposes, aka 'spamming' is forbidden, as is the on forwarding of chain emails.

14.8 Fraudulent Use of System IDs

Engaging in any activities where a user accesses or uses systems under another user's credentials is considered a major breach of security and may also be deemed fraudulent in law. Alleged misappropriation of another user's ID or access rights may result in a temporary revocation of access to all UCA IT Resources for those users who may be implicated in the alleged breach while such allegations are investigated.

User must not send e-mails or post items on virtual learning environments or social networking sites that purport to come from an individual other than the person actually sending the message.

14.9 Malware

Users must be careful not to perform any actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software (aka malware).

14.10 Unauthorised System Activities

Students are not allowed to monitor or intercept network traffic.

Students must not probe for the security weaknesses of systems.

14.11 Unauthorised Access

Users are forbidden to attempt to break into or damage computer systems or data held thereon. Attempts to access, or actions intended to facilitate access, to computers for which the individual is not authorised is not allowed.

Users must not use the University network for unauthenticated access to any other system or service.

Students must not connect unauthorised devices to the University network, without prior consultation with IT Services, except via the University's approved wifi connectivity services.

14.12 Commercial Activities

Commercial use of the University's internet access contravenes the acceptable use policy determined by the UK Education and Research Network Association and is not permissible. The use of UCA IT Resources must not be used in support of external voluntary or charitable activities unless express permission has been granted; there may be a charge for such usage.

The use of University business mailing lists without proper authorisation is forbidden.

The conduct of e-mail correspondence which could lead to the inadvertent formation of a contract binding upon the University must not be undertaken.

Users are not allowed to resell University or JANET services or information.

UCA IT Resources must not be offered for use to individual consumers or organisations outside the University except where such services support the mission of the University or are in the commercial interest of the University **and** have been granted permission by the Director of IT Services or the appropriate Executive Dean.

14.13 Frivolous Use

Non-academic activities which generate heavy network traffic or interfere with others' legitimate use of UCA IT Resources are not allowed.

15 Loss and Damage

Save as set out below, the University (including its affiliates, officers, agents and employees) accepts no liability to users for:

- Any loss or damage incurred by a user as a result of personal use of UCA IT Resources. Users should not rely on personal use of University electronic communications facilities for communications that might be sensitive with regard to timing, financial effect, privacy or confidentiality.
- For the acts or omissions of other providers of telecommunications services or for faults in or failures of their networks and equipment.
- Loss of data in the cloud.

The University does not exclude its liability under this Policy to users:

- For personal injury or death resulting from the University's negligence.
- For any matter which it would be illegal for the University to exclude or to attempt to exclude its liability.
- For fraudulent misrepresentation.

Users agree not to cause any form of damage to the University's IT facilities, or to any accommodation associated with them. Should such damage arise the University shall be entitled to

recover from such user, by way of indemnity, any and all losses, costs, damages and/or expenses that the University incurs or suffers as a result of such damage.

16 Health and Safety

The University strives to ensure that its facilities are used sensibly and responsibly and has a wide range of policies in these areas including such IT related policies on Display Screen Equipment, Accessibility.

17 Deletion of Data

Users should be aware that data deleted from local disks by the users, may still be accessible in some cases, via certain system tools.

Newsgroup articles, contributions to online bulletin boards, non-University owned mailing lists and emails once sent are stored on machines outside the jurisdiction of the University and in these cases withdrawal or deletion of these messages or emails may not be possible.

18 Back-up Services

The daily back-up process results in the copying of electronic data onto storage media that might be retained for periods of time and in locations unknown to the originator or recipient of electronic communications.

The practice and frequency of back-ups and the retention of back-up copies vary from system to system and are detailed in the Backup and Retention Policy.

Data can sometimes be susceptible to corruption due to hardware or software failure and users are encouraged to keep backups of their data. IT staff would make reasonable attempts to recover data however it might not be possible to do this in all situations.

19 Software and Hardware Auditing

The University has an obligation to ensure that only legal software is used on University owned equipment and to support this, appropriate technology may be used to audit all software that has been installed on University owned equipment without staff permission. Executive Deans, Heads of Department, Heads of School and the Director of IT Services may be notified of any illegal software discovered as part of the audit process.

20 Removal of Equipment

No equipment or other electronic communication facility may be borrowed, removed or moved from a designated location, without the explicit permission of the Director of IT Services, or other appropriately authorised member of staff.

No equipment can be taken out of the University premises without the explicit permission of the Directors of the Department, Heads of School, Executive Dean, or responsible owner as

appropriate. For permission to be granted the necessary forms detailing the purpose of the removal of the equipment and the equipment details must be filled by the applicant and countersigned by the appropriate manager or owner as mentioned above.

21 Telephone Systems

The Law protects the privacy of telephone conversations. Without court approval, it is illegal to record or monitor audio or visual telephone conversations without advising the participants that the call is being monitored or recorded.

The use of University telephone equipment creates transaction records (which include the number called and the time and length of the call) that are reviewed by University units as part of routine accounting procedures.

22 Investigation and Response to ICT violations

22.1 Policy

Instances of breaches may be drawn to the attention of the Director of IT Services via internal or external complaints, the intrusion detection system, or discovered in the normal course of business.

The actions taken because of a policy violation are dependent on the particular circumstances.

22.2 IT Services' Immediate Response

IT Services will determine the impact of the alleged violation and take, without notice, any necessary action if University resources and services are adversely affected to prevent immediate and further damage to the University network. Such actions may include:

- Suspension of an account
- Disconnection of systems or disable network ports
- Termination of running processes and programs
- Any other actions deemed necessary to restore network services.

22.3 Investigation of Alleged Violations

IT Services will gather evidence and provide information as directed by appropriate Heads of Departments and Schools to comply with any internal investigation. In some cases, the users may not be notified first or it may be required by law to provide the information without notifying the user. Investigations into complaints may necessitate the examination of systems and network activity logs and transaction logs. Contents of emails and other files will not be examined as part of a routine except in the following circumstances without the holder being notified:

- A court order requires that the content be examined and disclosed.
- The Director of IT Services is instructed in writing either by the Vice-Chancellor or the Registrar and Secretary as part of an internal investigation.

If the violation does not prevent other users from accessing network computer resources or result in a disciplinary procedure being instigated, the matter will be referred to the appropriate administrative authority for disciplinary action if the user refuses to comply.

Network access may be terminated immediately if the violation has been caused by an external entity with a contractual agreement with the University whilst the violation is investigated.

22.4 Reporting Security Incidents

All users of UCA IT Resources are encouraged to note and report any observed or suspected security incidents, security weaknesses in or threats to systems and services. Such reports can be made at the local campus helpdesks.

23 Disciplinary Action

Students whose actions contravene the guidelines within the UCA IT Acceptable Use Policy or any of its related policies will find themselves subject to disciplinary proceedings as defined within Student Regulations.

Individuals in contravention of the Acceptable Use Policy may also be subject to criminal proceedings. The University reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and / or other contraventions of this Policy.

CHECKLIST FOR STUDENTS CONSIDERING USING EXTERNAL ONLINE TECHNOLOGIES (WEB 2.0)

The University for the Creative Arts (UCA) encourages students to make appropriate use of external Web 2.0 technologies as long as adequate provision is made to ensure student and staff safety and privacy and minimise legal, operational, financial and reputational risk to the University.

Web 2.0 services offer attractive and useful applications services including blogs, wikis, office systems, social bookmarking and social networking. However, before using such services – or expecting others to do so – students should appreciate the issues outlined below:

Advantages

- External Web 2.0 technologies may offer the latest in functionality and support
- They may be used by a great many people (e.g. Facebook and Vimeo), making it easy to contact others and work together.
- Account creation and access is normally very quick and cheap, if not free
- They can help you to develop a professional portfolio of work for promotional purposes

Disadvantages

- It is easy to add content to such sites that you might later regret, as many such sites own control and will not always allow you to delete comments you no longer wish to be associated with.
- If you upload your work to a Web 2.0 provider you may be giving up some of your copyright and granting the service provider ownership of your work. If in doubt, check the terms and conditions of the service provider.
- Any content or comments you do submit can potentially become available to anyone in the world. It may also be unable for you to remove content and comments at a later date.
- Such content may have a longer life span than you might have imagined and could be accessed by a wide audience, including potential employers.

Always read and consider the terms and conditions for any service you register with and ensure that you understand the implications of the service conditions. Do not use the service for any university work unless you are happy with the terms and conditions; if you are in any doubt, ask your tutor for clarification.