Information Technology Policy

Last Reviewed: August 2017

Next Review Date: August 2018

Version Number: V1.1

1.0 Acceptable Use of IT

Policy Statement

This Acceptable Use Policy is intended to provide a framework for use of I.T. resources. It applies to all computing, telecommunication, and networking facilities provided at the college. It should be interpreted such that it has the widest application, in particular references to I.T. Services should, where appropriate, be taken to include departmental or other system managers responsible for the provision of an I.T. Service.

Users of commercial broadband services provided, or facilitated by, the College must abide by any specific policies associated with those services. Members of the College and all other users of the facilities are bound by the provisions of these policies in addition to this Acceptable Use Policy

The Systems Administrator is the Designated Authority within the College for all matters relating to the use of computer systems.

2.0 Use of IT facilities

I.T. resources are provided primarily to facilitate a person's essential work as a Staff or Student or other role within the College. No use of any I.T. service should interfere with another person's duties, studies, or any other person's use of I.T. systems, nor bring the College into disrepute, in any way.

Using College I.T. facilities in an office, library or laboratory, for non-work-related purposes, such as personal electronic mail or recreational use of the internet including social networking sites, are understood to enhance the overall experience of a staff or student but are not an absolute right. Priority to such facilities must always be granted to those needing facilities for academic work or other essential college business.

College e-mail addresses and associated e-mail systems must be used for all official college business, in order to facilitate auditability and institutional record keeping. All staff and students must regularly read their college e-mail.

Commercial work for outside bodies, using centrally managed services, requires explicit permission from the CEO and Systems Administrator; such use, whether or not authorised, may be liable to charge.

3.0 Privacy and Monitoring

It should be noted that designated IT Services staff, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files, stored on any computer, which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances, appropriately privileged staff will take all reasonable steps to ensure the privacy of service users. The College fully reserves the right to monitor e-mail, telephone and any other electronically mediated communications, whether stored or in transit, in line with its rights under the Lawful Business Practice regulations. Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services,
- prevent a breach of the law, this policy, or other college policy,
- investigate a suspected breach of the law, this policy, or other college policy,
- monitor standards.

Access to staff files, including electronic mail files, and/or individual I.T. usage information will not normally be given to another member of staff unless authorised by the CEO and Systems Administrator, or nominee. Such access will normally only be granted in the following circumstances:

- where a breach of the law or a serious breach of this or another college policy is suspected,
- when a documented and lawful request from a law enforcement agency such as the police or security services has been received,
- on request from Managers or co-workers of the individual require access to e-mail messages or files, which are records of a college activity, and the individual is unable, e.g. through absence, to provide them.

4.0 Behaviour

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the computer systems is, put at risk if users do not take adequate precautions against malicious software, such as computer viruses and associated malware. All users of I.T. services must ensure that any computer, for which they have responsibility, and which is attached to the college network, is adequately protected against viruses, through the use of up to date antivirus software (any exceptions to this must be approved explicitly by I.T. Services – (IThelp@lcuck.ac.uk), and has the latest tested security patches installed. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

Conventional norms of behaviour apply to I.T.-based media, just as they would apply to more traditional media. Within the College setting, this should also be taken to mean that the tradition of academic freedom will always be respected. The College, is committed to achieving an educational and working environment which provides equality of

opportunity, and freedom from discrimination on the grounds of race, colour, nationality, ethnic origin, gender, gender identity (transsexual), marital or civil partnership status, disability, including mental health difficulties, sexual orientation, religion or belief, age, social class, pregnancy or background.
Distributing material, which is offensive, obscene or abusive, may be illegal and may contravene College codes on harassment. Users of College computer systems must make themselves familiar with, and comply with, the College's HR policies.
No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.
Users of services external to the College are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Policy and be dealt with accordingly. This includes social networking sites, blog and wiki services and any other externally hosted services.

5.0 Acceptable and unacceptable behaviour

Unacceptable use of computers and network resources may be summarised as:

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law; propagation will normally be considered to be a much more serious offence;
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
- causing annoyance, inconvenience or needless anxiety to others;
- defamation (genuine scholarly criticism is permitted);
- unsolicited advertising, often referred to as "spamming";
- sending e-mails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address;
- attempts to break into or damage computer systems or data held thereon;
- actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software;
- attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;
- using the network for unauthenticated access;
- unauthorised resale of college services or information.
- excessive I.T. use during working hours that significantly interferes with a staff member's work, or that of other staff or students

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy (potential exceptions should be discussed with I.T. Services):

- the downloading, uploading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- the use of peer-to-peer software and related applications to illegally download and/or share music, video, film, or other material, in contravention of copyright law
- the publication on external websites of unauthorised recordings, e.g. of lectures;
- the distribution or storage by any means of pirated software;
- connecting an unauthorised device to the network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, I.T. policy, and acceptable use. This includes network hubs, switches and wireless access points not approved or managed by I.T. Services.
- monitoring or interception of network traffic, without permission;
- probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- associating any device to network Access Points, including wireless, for which you are not authorised;
- non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of I.T. services or which incur financial costs;
- excessive use of resources such as filestore, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- frivolous use of College owned computer laboratories, especially where such activities interfere with others' legitimate use of I.T. services;
- opening an unsolicited e-mail attachment, especially if not work or study-related;
- the deliberate viewing and/or printing of pornographic images;
- the passing on of electronic chain mail;
- posting of defamatory comments about staff or students on social networking sites;
- the creation of web based content, portraying official college business without express permission or responsibility;
- the use of college business mailing lists for non-academic purposes;
- the use of CDs, DVDs, and other storage devices for copying unlicensed copyright software, music, etc.;
- the copying of other people's web site, or other, material without the express permission of the copyright holder;
- Plagiarism, i.e. the intentional use of other people's material without attribution.

Disciplinary action may also be taken if casual or non-work related activity results in significant problems being caused for I.T. systems or services, arising for example from browsing non-work-related websites or the downloading of software containing malicious content.

Acceptable uses may include:

- personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others;
- advertising via electronic notice boards, intended for this purpose, or via other College approved mechanisms

However such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

7.0 Compliance with UK civil and criminal law

Users must comply with the provisions of any current UK law, including but not restricted to:

- intellectual property law, including laws concerning copyright, trademarks, and patents;
- the Computer Misuse Act 1990, and associated instruments;
- data protection laws;
- the interception and monitoring laws under the Regulation of Investigatory Powers Act 2000 (RIPA 2000); and
- the Terrorism Act 2000, the Terrorism Act 2006 and the Counter-Terrorism and Security Act (2015)

It should be noted that payment card information (credit/debit card numbers &c.) is personally identifiable and therefore falls in scope for data protection legislation, Accepting card payments also brings specific contractual obligations and no system or service for doing this should be procured without contacting the Finance or IT Services departments for specific advice.

Under the Lawful Business Regulations (LBR), IT Services would like to draw to the attention of all users the fact that their communications may be intercepted where lawful under RIPA 2000. IT Services also draws to the attention of all users the statutory obligation under the Counter-Terrorism and Security Act (2015) to have due regard to the need to prevent people being drawn into terrorism.

The Terrorism Act (2000) defines terrorism in section 1 of the Act.
Users must also comply with the terms of any licence agreement between the College and a third party, which governs the use of hardware, software or access to data.

The Data Protection Act 2018 applies to all personal identifiable information on all college systems and organised filing systems. All system users are required to handle such information in accordance with the information regulations.

Libel is a civil wrong, which, in proven cases, may incur substantial compensation. It is complex and therefore one of the easiest laws to contravene through ignorance. Facts concerning individuals or organisations must be accurate and verifiable and views or

opinions must not portray their subjects in any way that could damage their reputation. Check before publicly displaying contentious material.

IF IN DOUBT, DO NOT PUBLISH! Remember web pages, e-mail messages, tweets (etc) are covered by this legislation.

8.0 Security and confidentiality

Users must take all reasonable care to maintain the security of computing facilities and files to which they have been given access. In particular, users must not transfer passwords, or rights to access or use computing facilities, without appropriate authority from the relevant Dean of College or Director of Service or nominee or authorised officer. The confidentiality, integrity and security of all personally identifying data held on systems must be respected, even where users have been authorised to access it.

Users must ensure that a pin protects portable devices containing College information or similar mechanism, whether the College purchased the device, is personally owned or belongs to a third party.
Users with information deemed to be secret or confidential, are required to take additional security measures proportionate to the sensitivity of the information concerned. Prior to terminating their relationship with the College, users must make appropriate arrangements for the return, destruction or other disposition of any College computer, equipment or data in their possession. Users must ensure the safe disposal of any College data when disposing of computer equipment, including personally owned devices.

The End