University of Central Lancashire

Rules for the Use of IT Facilities

Effective September 2017 - August 2018

STUDENT REGULATIONS AND POLICIES

uclan.ac.uk/studentcontract

Contents

1 INTRODUCTION

These Rules set out the standards to be observed by members of staff, students, and other persons or bodies, when using the University's IT Facilities.

The purpose of the Rules is to ensure that all use is of a good quality, and does not breach any relevant statutory or legal obligation or any of the University's own regulations. The University wishes to encourage responsible use of its IT Facilities for appropriate purposes, and wishes to prevent the use of the University's IT Facilities for purposes, which are unlawful, or cause annoyance or inconvenience to others.

No User should act in a way that might endanger the good name or reputation of the University. All Users must therefore ensure that any material placed on the IT Facilities or any use of the IT Facilities does not risk criminal prosecution or civil legal action. Even if the material is legal or the use is legal, it still must not be such that it might endanger the good name or reputation of the University or might bring the name of the University into disrepute.

The use by any User of the IT Facilities implies acceptance on the part of that User of these Rules together with the IT Security Policy and the policies referred to within these documents as applicable.

1.1 MONITORING COMPUTER USAGE

Access to IT Facilities is restricted to authorised Users only, and such authority is formally assigned on each IT system. On certain public facing systems, such as the University's website, a person accessing these systems automatically becomes an authorised User for the purposes of the Rules.

Computer usage is logged and the University reserves the right to monitor and access any information on the IT Facilities or on equipment connected to the IT Facilities or on computer media used with the IT Facilities for any of the following reasons:

- Record keeping purposes
- Checking compliance with the University's regulations and procedures
- Quality control or staff training
- Preventing or detecting crime
- Investigating or detecting the unauthorised use or misuse of the IT Facilities
- Checking for viruses and cyber attacks
- Reasonably dealing with other threats to the IT Facilities

2 INTERPRETATION

For the purpose of these Rules, the following words and phrases have the following meanings:

- "LIS": means the University's Learning and Information Services
- "The Rules": means the Rules governing the use of the IT Facilities at the University
- "The IT Facilities": means the University's computers, computing systems, operating systems, software, IT network/wireless infrastructure, Hosted IT Service providers including but not limited to; Office 365 services, LIS Customer Support Helpdesk (Assyst), Library Catalogue System (Ex Libris)

- "the University": means the University of Central Lancashire.
- "User or Users": means any person, firm, company or organisation granted authorisation to use the IT Facilities.
- "the Web": means the computer system known as the World Wide Web which is to be used as the system for disseminating, viewing and retrieving information through the IT Facilities including electronic mail, file transfers and remote log ins.
- "Uploaders": means those members of staff whose designated role as an Uploader with regard to the World Wide Web is to upload files on to the World Wide Web through the IT Facilities.
- “Extremism” has the meaning provided by the statutory Guidance for specified authorities in England and Wales on the duty in the Counter-Terrorism and Security Act 2015 to have due regard to prevent people from being drawn into terrorism. This means vocal or active opposition to fundamental British values, including: democracy; the rule of law; individual liberty; mutual respect and tolerance of different faiths and beliefs; and the call for the death of members of the armed forces.

3 RESPONSIBILITIES OF ALL USERS OF THE IT FACILITIES

All Users must:

- Only use the University’s IT Facilities in accordance with the IT Security Policy, the Data Protection Code of Practice and the FOI Policy and Procedures (see Schedule A).
- Only use the University’s IT Facilities (including software) for permitted uses, which are restricted to the educational purposes, listed below.
- Not use the University’s IT Facilities for any use which is prohibited or otherwise in breach of these Rules

4 PERMITTED USES

Permitted uses include:

- Teaching;
- Research authorised by the University;
- Personal educational development and administration;
- Management of the University's organisation and business;
- Development work associated with any of these is also permitted

5 PROHIBITED USES

Prohibited uses include, but are not limited to:

- Placing on the IT Facilities or transmission of material which is by its nature or effect a commercial advertisement or other unsolicited transmission to a mass-mailing list (unsolicited bulk email or "spam"), other than a commercial advertisement on behalf of the Students' Union, or the University's trading companies
- Consultancy and commercial exploitation
- Use of the Internet and e-mail, use of chat rooms, etc. which does not relate to the University's educational purposes
- The playing of recreational computer games
- Harassment of others by inappropriate use of the IT Facilities
- Maliciously interfering with the IT Facilities or any other computer system or network
- Attempting to gain or successfully gaining access to any computer system, network or account without the required permission or otherwise where it is not intended the User may have such access
- Probing the security of any computer system, network or account
- Viewing, modifying or otherwise tampering with any data or computer system without consent or where it is otherwise not intended the User should do so

6 INFORMATION HANDLING AND STORAGE ON IT FACILITIES

Regulations on how all information must be accessed, handled and stored on University IT Facilities and how the information relating to the University's organisation and business must be processed can be viewed in the IT Security Policy.

Users must not use the IT Facilities for the creation, display, storage or transmission of any of the following material:

- Material, which is offensive, obscene or excessively violent, and in particular material which may lead to injury or damage to minors.
- Material which discriminates or encourages discrimination on any prohibited grounds namely disability, age, sex, race, gender, sexual orientation, marriage & civil partnership, gender reassignment and pregnancy & maternity.
- Material which is in breach of the provisions of any legislation from time to time in force in the UK (see Schedule B below)
- Material related to proscribed organisations or material that could be considered to be at risk of drawing people into terrorism and/or material that could be described as extremist and poses a risk of inducing people into making the transition from extremism to terrorism.
- **Material, which might contravene the law of defamation. Users must therefore ensure that facts communicated to others relating to individuals or organisations are accurate and verifiable. Any views or opinions expressed by Users must not damage the reputation of those persons or individuals who are the subject of those views, and must accurately reflect only the honest and reasonably held opinion of the User.**

Users of the IT Facilities must not use University IT facilities for the display, storage or transmission of material, which the User either knew, or ought to have known, would breach confidentiality obligations to the University or another person or organisation.

If such usage is required for properly supervised and lawful research purposes, the Director of Learning and Information Services, or nominee, must give prior approval to such usage following an application made through the User's Head of School.

7 PASSWORDS

All users of the University IT Facilities must access information held on those facilities by the use of passwords as detailed in the IT Security Policy.

- The User's password should be known only to the User and the IT system (The University will not issue any communications that will request you to supply your password).
- The User must not communicate their passwords to a third party.
- The User must not allow their disk space or any other IT Facility to be used by anyone else using their personal user account.
- The User must immediately inform LIS if they think that any other person has obtained unauthorised access to their system.
- The User should change their password at regular intervals.

8 WORLD WIDE WEB

Users must identify themselves as being the authors of any material or information which they place on the Web, or which an Uploader places on the Web on their behalf. Users acting as Uploaders for all the authors in a School or Service are not required to read or edit the files processed by them in this capacity and are not required to accept responsibility for the contents of files which they place on the Web in their capacity as an Uploader, such responsibility remains with the author(s). Uploaders should however ensure that all material they place on the Web contains the author's details.

Authors are responsible for the content, accuracy and currency of all information identified as written by them on the Web and must ensure that any entries on the Web are with the permission of the owner or as otherwise permitted by law or the terms of any copyright licences.

So far as is reasonably practicable, Users should remove from the Web any files under their control which contain out-of-date information. In any event, Users must display the date when each page of information was last updated and ensure that each page of information conforms generally to the University's design guides for authors.

Students must comply with the University Code of Practice for Personal Internet Presence as detailed in Schedule C.

9 DATA PROTECTION AND COPYRIGHT

Users shall not breach the privacy of any information held by the University on its IT Facilities or incite another to so do. Personal data (as defined by the Data Protection Act 1998) may only be held or processed on the IT Facilities in accordance with the provision of the Act and the uses permitted by the University (see section 4 above). The general principles of the Act are set out in the University's "Data Protection Code of Practice" and all Users of the IT Facilities should familiarise themselves with the content of this document.

Users may only copy, modify, disseminate or use any part of any information or material belonging to another user, including another user's e-mail address, with the permission of the owner or as otherwise permitted by law or the terms of the copyright licences.

10 EMAIL

Users are not permitted to send global emails i.e. emails to mass mailing lists, including the University's email address book (without special permission, in the case of students or staff, from the Director of Learning and Information Services, or nominee). Please see the Email Use Policy for further rules relating to emails.

Other rules governing the use of external e-mail accounts and the storage of corporate data are included in the IT Security policy.

Any breach of the Email Use Policy may be subject to sanctions as set out in section 14 below.

11 HARDWARE/NON-STANDARD HARDWARE AND IT FACILITIES

All users of the IT Facilities must adhere to the statements in the IT Security Policy:

- Users must not connect any equipment to the IT Facilities without prior permission from the Director of Learning and Information Services, or nominee.
- Users must not damage, disconnect or tamper with computing equipment, its systems programs, or other stored information.

12 SOFTWARE/NON-STANDARD SOFTWARE AND IT FACILITIES

All users of the IT Facilities must adhere to the statements in the IT Security Policy:

- Where a User's queries or requests for support have to be taken up with a supplier of hardware or software, this must be done through a single contact within LIS.
- Software used on University IT Facilities must not be copied without express written permission of the Director of Learning and Information Services, or nominee, and appropriate written declarations signed by the User.

13 Access to Data Hosted by External Suppliers

When external providers supply data access to the University, then availability and use of that data by members of the University is subject to the requirements of such agreements, contracts and licences as may be applicable.

14 Breach of The Rules

14.1 Sanctions

In the event of any breach of these Rules then the University may apply one or more of the following sanctions:

- Withdrawal of the information concerned from the University's IT Facilities.
- Temporary or permanent prevention of access to the relevant pages on the Web.
- The withdrawal of the User's right to use the IT Facilities for a specified period.
- The University's Regulations for the Conduct of Students may be invoked. In the case of an apparent breach of the Rules by a member of University staff his/her Head of School/Service will be informed. Further action may be taken in accordance with University procedures set out in the Staff Handbook.
- In the case of staff, the appropriate University HR procedures may be invoked.

Users should note that breaches of the provisions set out in these Rules may also lead to criminal or civil prosecution.

The University reserves the right to withdraw a student's right to access the IT Facilities in the event that tuition fees are outstanding, in accordance with the Tuition Fees Policy.

14.2 Procedure

If a breach is sufficiently serious, the University reserves the right to refer straight to a particular stage in the procedure before a verbal warning has been given and/or without reference to the prior stages where this is reasonable and proportionate in light of the severity of the breach concerned.

14.2.1 Initial Action

LIS staff will normally seek to resolve breaches of these Rules in an informal manner. Where the breach is minor in nature, the user will initially be given a verbal warning. If the user continues to breach the Rules notwithstanding the warning, and/or the severity of the breach so justifies, the user (student or external), may be denied access to the IT Facilities for a period of up to 7 days.

Whenever students are denied access to the IT Facilities for disciplinary reasons, their Head of School will be informed.

If a breach of rules takes the form of or is accompanied by noisy, disruptive, or violent behaviour, the user may be obliged to surrender his/her UCLan card and be escorted from University premises. In such a case the matter may be referred for action under the Regulations for the Conduct of Students.

Individuals who feel aggrieved by action taken against them may appeal to the Director of Learning and Information Services, or nominee.

14.2.2 Further action

If an alleged breach is sufficiently serious, or becomes so by repetition or because of an uncooperative response to warnings, further action may be taken as follows:

a) Students

A student will be called to see a senior member of LIS and other members of LIS staff may also be present. A friend may accompany the student to this meeting, and a member of academic staff may be present, if appropriate. Others may be asked to attend such meetings as witnesses.

If a breach of the Rules is established, the student will be warned about future conduct and may be denied access to the IT Facilities for up to 14 days. The student will also have his/her name recorded within LIS for a period of one year from the date of the offence; the outcome of the meeting will be communicated to the Director of Learning and Information Services, or nominee, and a student's Head of School/Course Leader. Any further breach of these Rules which occurs during that year may result in withdrawal of access to the IT Facilities for up to 30 days or referral to the student's Head of School in accordance with the Regulations for the Conduct of Students.

Any appeal arising from this procedure will be to the Director of Learning and Information Services, or nominee.

Particularly serious cases, or repeated breaches of the Rules, may be referred to the student's Head of School to be dealt with in accordance with the University's Regulations for the Conduct of Students, in which case access to the IT Facilities may be withdrawn until the completion of disciplinary procedures.

b) External users, including non-members

External users will be seen by a senior member of LIS staff who may provisionally remove their access rights to all the IT Facilities with immediate effect. This action may subsequently be confirmed and extended indefinitely by the University. Any fees paid will not be returned.

14.3 Procedure to apply to staff users

The relevant sanctions will be applied in accordance with the Staff Handbook.

15 APPENDIX A - SUPPORTING DOCUMENTATION

These rules for the use of the University's IT Facilities should be read in conjunction with the University Information Management Guide which in addition to the use of the IT Facilities details the University's rules, policies and codes of practice relating the following areas of information management:- IT Security Policy

Use of Library Facilities

Data Protection Code of Practice

Freedom of Information Policy and Procedures

Email Use Policy

The Acceptable Use Policy of JANET (Joint Academic NETwork)

https://community.jisc.ac.uk/library/acceptable-use-policy The

above (except for the final policy) are all available at

https://www.uclan.ac.uk/students/life/rules_regs.php

Users shall not breach the privacy of any information held by the University on its IT Facilities or incite another to so do. Personal data (as defined by the Data Protection Act 1998) may only be held or processed on the IT Facilities in accordance with the provision of the Act and the uses permitted by the University (see section 4 below). The general principles of the Act are set out in the University's "Data Protection Code of Practice". and all Users of the IT Facilities should familiarise themselves with the content of the said documents.

Users may only copy, modify, disseminate or use any part of any information or material belonging to another user, including another user's e-mail address, with the permission of the owner or as otherwise permitted by law or the terms of the copyright licences.

16 APPENDIX B - RELATED LEGISLATION

Use of the IT Facilities is subject to all relevant laws, including but not limited to the laws of copyright and libel, the Computer Misuse Act 1990, the Malicious Communication Act 1988 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

The IT facilities must not be used to store, process or access any information that is in breach of the provisions of any legislation from time to time in force in the UK, including, without prejudice to the generality of the foregoing:

- The Official Secrets Act 1989
- The Data Protection Act 1998
- The Race Relations Act 1976
- The Sex Discrimination Act 1986

- The Disability Discrimination Act 1995
- The Computer Misuse Act 1990
- The Malicious Communications Act 1988
- The Copyright (Computer Programs) Regulations 1992
- The Criminal Justice and Public Order Act 1994
- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Communications Act 2003
- The Digital Economy Act 2010
- The Equality Act 2010
- The Defamation Act 2013
- The Counter-Terrorism and Security Act 2015 and associated statutory guidance and any statutory re-enactments or modifications thereof, or regulations made thereunder or material which does not comply with the British Code of Advertising, Sales Promotion and Direct Marketing of the Advertising Standards Authority from time to time in force.

17 Appendix C Code of Practice for Personal Internet Presence

17.1 Scope and Purpose

- This Code of Practice applies to all students admitted or enrolled by the University to follow a programme of studies.
- For the purpose of this Code of Practice, 'Personal Internet Presence' is defined as all internet presence including: e-mail usage, participation in online communities and hosted services (such as social networking sites and forums), and maintaining personal profiles or pages (such as blogs).
- This Code of Practice is designed to bring students' attention to the measures within the University, which are designed to protect them from electronic abuse or harassment by a fellow student, to protect the reputation of the University, and to inform them of the local rules governing internet use.

17.2 Guidance

- Normally, where a student's internet presence does not make any reference to the University then the content is of no concern to the University; however, the University retains the right to investigate any inappropriate internet usage.
- If a student wishes to refer to the University, its staff and/or students, information posted should comply with the Rules for the Use of IT Facilities, the IT Security Policy and this Code of Practice.
- If maintaining a personal internet presence from a University workstation, a student must comply with the Rules for the Use of the University's IT Facilities and the IT Security Policy.

- Students may not brand external webpages with the University's identity or logo, or otherwise appear to represent the University. The Advancement Service maintains a University branded internet presence, and if you wish to get involved in those pages you can liaise with this team.
- If a student is contacted about posts on his/her site which relate to the University by individuals external to the University, s/he should discuss it with staff in advance before responding.
- If a student breaks the law on his/her site (for example by posting something defamatory), s/he will be personally responsible.

17.3 Rules Governing Personal Internet Presence

Students are expected to conduct themselves at all times in a manner which demonstrates respect for the University, its staff, students and property. The following list is indicative of types of online misconduct but is not intended to be exhaustive:

- Deliberately disclosing privileged or confidential information about the University, its staff or students. This might include details of internal University discussions;
- Using a site to attack or abuse University staff or students;
- Disrespecting the privacy and/or the feelings of others;
- Including personal details or pictures etc. of other students without their prior permission;
- Electronically distributing or publishing a post, notice, sign or publication of material of any nature which is threatening, abusive, insulting, obscene or offensive, or constitutes harassment or is illegal or makes other fear violence;
- Presenting violent, incident, disorderly, aggressive, threatening or offensive images or language towards a member of the University community.