University of Central Lancashire

Rules for the use of the IT Facilities

Effective April 2016 to August 2017

STUDENT REGULATIONS AND POLICIES

uclan.ac.uk/studentcontract

INFORMATION MANAGEMENT GUIDE
RULES FOR THE USE OF THE UNIVERSITY'S IT FACILITIES
("The Rules")

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 the same, 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 and of all other relevant rules, regulations and procedures produced, and adopted, from time to time by the University.

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 Regulations
- quality control or staff training
- preventing or detecting crime
- investigating or detecting the unauthorised use or misuse of the IT Facilities
- checking for viruses
- other threats to the IT Facilities

2 Interpretation

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

1) “LIS”: means the University’s Learning and Information Services

2) “The Rules”: means the Rules governing the use of the IT Facilities at the University

3) “the IT Facilities”: means the University’s computers, computing systems, operating systems and software.

4) "the University": means the University of Central Lancashire.

5) "User or Users": means any person, firm, company or organisation granted authorisation to use the IT Facilities.

6) "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.

7) "Up-loaders": means those members of staff whose designated role as an Up-loader with regard to the World Wide Web is to up load files on to the World Wide Web through the IT Facilities.

8) “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 form 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 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, the Copyright Code of Practice and the FOI Policy and Procedures.
- Only use the University's IT Facilities (including software) for permitted uses which are restricted to the educational purposes listed below

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 (although the supplier may allow such use for an agreed fee)
- Work of significant benefit to employers of students on industrial placement and employers of part-time students
- Non-educational use of the Internet and e-mail, use of chat rooms, etc
- The playing of recreational computer games
- Harassment of others by inappropriate or excessive 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 racial or ethnic grounds, or which is likely to incite racial or ethnic discrimination.

- Material which discriminates or encourages discrimination against any person on the grounds of gender, sexual orientation, disability, or religion or belief.

- Material which is or likely to be in breach of the provisions of any legislation from time to time in force in any jurisdiction (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 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 the same 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 their 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 these facilities by the use of passwords as detailed in the IT Security Policy Section 14 User Identification and Authentication Use of Passwords, and Section 16 Use of Computers

1) 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).
2) The User **must not** communicate their passwords to a third party.
3) The User **must not** allow their disk space or any other IT Facility to be used by a third party.
4) The User **must** immediately inform LIS if they think that any other person has obtained unauthorised access to their area.
5) The User should change their password at regular intervals.

8 World Wide Web

1) Users must identify themselves as being the authors of any material or information which they place on the Web, or which an Up-loader places on the Web on their behalf. Users acting as Up-loaders 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 Up-loader, such responsibility remains with the author(s). Uploaders should however ensure that all material they place on the Web contains the author's details.
2) Authors are responsible for content, accuracy and currency of all information 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 the copyright licences.
3) 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.

9 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).

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

10 Hardware/Non Standard Hardware and IT Facilities

All users of the IT Facilities must adhere to the statements in the IT Security Policy No 9 Network Management/Protection Controls Prohibition of Non Standard Hardware and Software

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

11 Software/Non Standard Software and IT Facilities

All users of the IT Facilities must adhere to the statements in the IT Security Policy No 9 Network Management/Protection Controls Prohibition of Non Standard Hardware and Software and No 16 Use of Computers – Software

1) Where User queries and 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.
2) 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.

12 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.

13 Breach of the Rules

13.1 In the event of any breach of these Rules then the University may exercise 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 and Library Facilities.
- Appropriate disciplinary action. In the case of students of this University, the University's Regulations for the Conduct of Students may be invoked. The procedure below shall apply to non staff Users. 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.
- The above list of sanctions is not exhaustive, and may be altered or augmented by the University, depending upon the nature of the breach.
- Users should note that breaches of the provisions set out in these Rules may lead to criminal or civil prosecution.

13.2 Procedure to apply to non-staff users

13.2.1 Initial Action

LIS staff will normally seek to resolve breaches of these Rules in an informal manner.

In cases of apparent breaches of the Rules a User student or external may be denied access to the IT Facilities, his/her Library borrower rights may be withdrawn, and an incident report form may be completed, prior to a meeting with a senior member of LIS staff. Failure to attend such a meeting within a calendar month will result in additional disciplinary action. Users are advised that, even though they may not be in breach of these Rules or in debt specifically to LIS, they may also be denied access to the IT Facilities and their Library borrower rights may be withheld at the request of Financial Services, pending payment of moneys owing to the University. Whenever students are denied access to the IT Facilities and their borrower rights are withheld 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 corporate card and be escorted from University premises.

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

13.2.2 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:

13.2.3 Students

A student will subsequently be called to see a senior member of LIS in the first instance 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 and all Library Facilities for up to five working 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 appeal arising from this procedure will be to the Director of Learning and Information Services, or nominee. Any further breach of these Rules which occurs during that year may result in the withdrawal of access to the IT Facilities and Library facilities for up to 10 days or in referral to the student's Head of School in accordance with the Regulations for the Conduct of Students.

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 the University's *Regulations for the Conduct of Students*, in which case access to the IT Facilities and access to Library Facilities may be withdrawn until the completion of disciplinary procedures.

13.2.4 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 and Library Facilities with immediate effect. This action may subsequently be confirmed and extended indefinitely by the University. Any fees paid will not be returned.

SCHEDULE 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***
  https://www.uclan.ac.uk/students/it/files/appendix_e_it_security_policy.doc

- ***Use of Library Facilities at all sites***
  https://www.uclan.ac.uk/students/library/library_rules.php

- ***Data Protection Code of Practice***
  https://www.uclan.ac.uk/information/services/sds/dpa_foia_management/DP_code_of_practice.php

- ***Freedom of Information Policy and Procedures***
  https://www.uclan.ac.uk/information/services/sds/dpa_foia_management/foia.php

- ***Copyright Code of Practice***
  https://www.uclan.ac.uk/students/library/code_practice.php

- ***The Acceptable Use Policy of JANET (Joint Academic NETwork)***
  http://www.ja.net/company/policies/aup.html

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 should familiarise themselves with the University's Copyright Code of Practice.
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.

SCHEDULE 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 or is likely to be in breach of the provisions of any legislation from time to time in force in any jurisdiction 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 Counter-Terrorism and Security Act 2015 and associated statutory guidance

and any statutory re-enactments or modifications thereof, or regulations made there under, 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.

Responsibility for Review

The Director of Learning and Information Services is responsible for the maintenance and annual review of these Rules.

These Rules are subject to change from time to time. They form part of a suite of rules and regulations that pertain to students and are cited in the Student Guide to Regulations issued to all new students. Copies of the Rules are displayed in all University libraries; a copy will be provided to any user on request. The Rules are published on the LIS pages on the University's Web site at

https://www.uclan.ac.uk/students/it/files/it_facilities_rules.doc