LONDON'S GLOBAL UNIVERSITY

Computing Regulations

Acceptable Use Policy
Information Security Policy
Supporting Policy 2

University College London

Document Summary

Status	Approved
Information Classification	Public
Document Version	Approved by the Information Risk Governance Committee 29-Nov-2021

University College London, Gower Street, London WC1E 6BT
Tel: +44 (0)20 7679 2000
www.ucl.ac.uk

1. Introduction

1.1 Purpose

UCL depends heavily on its Information Technology (IT) services for its research, teaching and administrative activities. These services are funded on condition they are used for legitimate, authorized purposes, and UCL may be required from time to time to demonstrate to external auditing bodies that it has mechanisms in place to manage, regulate and control them. The main purpose of these regulations is to define what constitutes acceptable use; to encourage the responsible use of facilities; to maximize the availability of resources (equipment, infrastructure and staff) for legitimate purposes; and to minimize the risk of misuse from inside or outside UCL.

These regulations incorporate the acceptable use policy of our service provider, JISC (Joint Information Systems Committee), which manages network connections between Universities and Colleges and the Internet (the JANET Network). The full text of their policy can be found at: ***https://community.jisc.ac.uk/library/acceptable-use-policy***

There are also various national and European Union laws and directives that govern the use of IT, and others that make explicit reference to IT. These are mentioned in more detail later. UCL has a duty to bring these to the attention of its staff and students.

If you are not sure whether something you are planning to do might contravene these regulations, check first with your line manager (in the case of staff) or tutor (in the case of students), or seek help from the ISD Service Desk before proceeding.

1.2 Scope

These regulations cover the use of all IT services and facilities provided by UCL or by third parties on behalf of UCL. For the purposes of clarification, these include, but are not limited to:

a. all devices irrespective of ownership when connected to the UCL communications network;

b. services run by Information Services Division (ISD) which may be used by any member of UCL. All users of these services must be registered with ISD;

c. services run by the ISD Application Services team which may be used by authorized, registered members of UCL;

d. services run by the Library and administrative divisions of UCL;

e. services run by other parts of UCL;

f. facilities and systems operated by departments for academic research, teaching and administration. Arrangements for use of these facilities are made through the department concerned and are normally restricted to its own staff and students;

g. content hosted on UCL's IT facilities which is accessible via the internet by members of the public;

h. {This point has been removed} [1]

i. services operated by third parties.

Software obtained under an educational licence agreement may also be subject to the terms of these regulations (see, for example, section 3.1 below). They do not, however, apply to other organisations whose traffic UCL relays by formal arrangement (such as the JISC 'sponsored' sites), unless the terms of an arrangement stipulate otherwise. In the case of sponsored sites, regulations will be established by agreement.

2. Authorized Use

In these regulations "authorized use" is defined as:

a. for students, use properly associated with the UCL programme of study or course for which a student is registered; and reasonable personal use;

b. for employees, use in the course of or properly and directly associated with their employment; and reasonable personal use;

c. for honorary staff, use properly associated with their appointment; and reasonable personal use;

d. for trades union business and UCLU societies, use properly associated with union or society activities;

e. for users who are neither staff nor students, use restricted to those purposes specified in the case made for registration.

Reasonable personal use is defined as incidental and occasional use which does not:

a. disrupt or distract the individual from the efficient conduct of UCL business (i.e. due to volume, frequency, time expended or time of day used);

b. involve accessing, downloading, storing or sending offensive or inappropriate material or information, or is such as to amount to a criminal or civil offence examples of which are listed in Regulation 3(d);

c. restrict the use of those systems by other legitimate users;

d. risk bringing UCL into disrepute or placing UCL in a position of liability;

e. add significantly to running costs and

f. breach the Regulations set out in paragraph 3

[1] {This point has been removed} since UCL Union is separate and distinct from UCL - [SWG 07-11-2016]

Any use that falls outside of these definitions is prohibited and may lead to UCL disciplinary procedures being invoked, with penalties that could include suspension from the use of all UCL computing facilities for extended periods. Serious cases may lead to disciplinary action, up to and including dismissal without notice and may expose you to court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against UCL and any legal action to which UCL is, or might be, exposed as a result of your unauthorized use.

3. Regulations

3.1 IT users must:

a. respect the copyright of all materials and software that are made available by UCL service providers and third parties for authorized use;

   Users must not make, run or use unlicensed copies of software or data. They should only download data or datasets where they are explicitly permitted to do so. They must abide by the User Acknowledgement of Third Party Rights, the terms of the JISC Model Licences (see ***https://subscriptionsmanager.jisc.ac.uk/about/guide-to-model-licence***), Copyright Law (Copyright, Designs and Patents Act 1988) and by any specific conditions of use imposed by the owners or suppliers of software or data. In particular users should be aware that, unless otherwise stated, software and datasets provided by UCL should only be used for UCL educational purposes.

b. familiarize themselves with and comply with the requirements of the Data Protection Act and UCL policy, most especially the obligation to notify UCL's Data Protection Officer of any relevant data holdings (see ***https://www.ucl.ac.uk/data-protection/data-protection-overview/understanding-data-protection-ucl***)

c. comply with the Computer Misuse Act 1990 which makes activities such as hacking or the deliberate introduction of viruses and other malware a criminal offence;

   Hacking is defined here as the unauthorized access or modification of a computer system (locally or through a network), or the use of resources that have not been allocated, with intent to access, modify or damage another's files or system files, or to deny service to legitimate users, or to obtain or alter records, or to facilitate the commission of a crime.

d. have the written approval of their Head of Department where activities which might be subject to legislation are carried out in pursuit of legitimate, approved academic research (for example, work involving the use of images which may be considered obscene or indecent, or research into computer intrusion techniques)

e. take all reasonable precautions to prevent the introduction of any virus, worm, Trojan Horse or other harmful program to any computer, file or software;

f. comply with local arrangements for booking public clusters and machines in public clusters.

3.2 IT users must not:

a. use material or programs in a way which is unlawful, defamatory or invasive of another's privacy;

b. use the IT services and facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data;

c. use the IT services and facilities in a way which infringes any patent, trademark, trade secret, copyright, moral right, confidential information or other proprietary right of any third party

d. jeopardize the provision of services (for example by inappropriate use of bulk e-mail, or by recreational use that deprives other users of resources);

e. publish, create, store, download, distribute or transmit material that is offensive, obscene, indecent or unlawful. Such materials will always include, but at UCL's discretion may not be limited to, items deemed to be offensive, obscene, indecent or unlawful under current UK legislation;

f. use IT facilities in a way that brings or could bring UCL into disrepute. This includes associating UCL with external facilities such as Web sites that could bring UCL into disrepute by association, for example by embedding UCL email addresses in such sites, or by providing hyperlinks from UCL web sites to such sites;

g. disclose or share credentials e.g. password to others, or use accounts or passwords belonging to others, or otherwise to circumvent registration procedures;

   The term "password" is here taken to refer to any authentication credential issued by UCL, and includes both hardware tokens and cryptographic keys. Users will be held personally liable and may be subject to disciplinary proceedings for any misuse of their account resulting from the disclosure of passwords to others.

h. access or attempt to access any data processing systems or services at UCL or elsewhere for which permission has not been granted, or facilitate such unauthorized access by others;

i. attempt to circumvent any firewall or software designed to protect systems against harm;

j. interfere or attempt to interfere with or destroy systems or software set up on public facilities (this includes loading or attempting to load unauthorized software on to any UCL IT facilities);

k. interfere with, disconnect, damage or remove without authority any equipment made available for use in conjunction with any UCL IT facilities;

l. set up equipment to provide services that they are not competent to administer, especially if such services result in security vulnerability or exposure to misuse;

m. use mobile phones, smoke, eat or drink in public cluster rooms;

n. interrupt teaching sessions when a cluster room has been booked for this purpose.

UCL does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed via any UCL IT system or via the Internet. You may not store on or transmit from any system any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability. [Please also bear in mind the UCL policy on discrimination and harassment.]

Breaches of this policy will lead to disciplinary action. In the event that you receive or become aware of obscene, indecent, offensive, inflammatory, discriminatory or socially offensive material, you should notify the relevant person set out in paragraph 5.2.

Failure to comply with these regulations may lead to disciplinary action, up to and including dismissal from UCL without notice and may expose you to court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against UCL and any legal action to which UCL is, or might be, exposed as a result of your unauthorized use.

4. Conditions of Use

Use of UCL IT facilities is subject to the following conditions. Additional conditions may apply to locally managed systems; it is the responsibility of those managing such systems to make their users aware of any local regulations.

4.1. The facilities (including software) are provided entirely at the risk of the user. UCL will not be liable for loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), damage (including damage to hardware, software or data) or inconvenience arising directly or indirectly from the use of the facilities, except where statutory health or safety matters are involved.

4.2. Whilst UCL's information security policy requires providers of computing facilities to employ appropriate security measures to prevent unauthorized access to, alteration, disclosure, destruction or accidental loss of personal and other data, UCL cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other. The same applies to any other electronic material submitted to or processed on facilities provided or managed by UCL or otherwise deposited at or left on its premises.

4.3. UCL accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or the invalidation of any warranty agreement) to equipment not owned by UCL as a consequence of any work carried

out on such equipment by members of staff (or students acting in the capacity of members of staff), whether authorized or not.

4.4. UCL accepts no liability for any loss (including any loss of software, data or other computer functionality or any economic, consequential or indirect loss), or damage (including damage to hardware, software or data or invalidation of any warranty agreement) to equipment not owned by UCL as a consequence of direct or indirect connection, whether authorized or not, to UCL networks. The user shall indemnify UCL for any loss or damage, whether direct or indirect, malicious or inadvertent, suffered or incurred as a consequence of the interconnection of any hardware or software not owned by or under the control of UCL with any IT system, hardware, software or data owned or controlled by UCL.

4.5. UCL reserves the right to inspect, monitor, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse. Your use of IT facilities provided by UCL is governed by current UK legislation.

Any monitoring of systems or networks may be carried out **only** in accordance with the UCL Policy on Monitoring Computer and Network Use, ***https://www.ucl.ac.uk/informationsecurity/policy/policy/public-policy/Monitoring***

For the avoidance of doubt, this does not preclude third parties who operate services on behalf of UCL from carrying out lawful monitoring and disclosure on their systems and networks.

Related information can be found at ***http://www.ucl.ac.uk/privacy****. It is important to be aware that communications on* or *through UCL's computer systems may be monitored or recorded to secure effective system operation and for other lawful practices. For example, monitoring of user accounts might occur if UCL has reason to believe that its computer facilities were being misused to send unsolicited commercial e-mail.*

4.6. UCL reserves the right to check for insecure and vulnerable systems and to block access to systems and/or services (ports) which place at risk the integrity of its network or services, or which may pose a threat to third parties.

4.7. UCL reserves the right to disconnect poorly managed equipment from the departmental LAN, or in extreme cases disconnect the departmental LAN from the UCL network until the offending machine is disconnected or shown to be configured correctly.

4.8. Any form of electronic communication may be construed in law as a publication and UCL publishing guidelines will apply. Users must be aware of the implications with respect to Intellectual Property Rights of publishing information in any electronic

form. For further information, consult the UCL Library Services guidance at ***http://www.ucl.ac.uk/library/copyright/your-own-copyright***

5. Procedures for dealing with misuse or suspected security violations

5.1. In the event of suspected misuse of IT facilities UCL reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. UCL may also disconnect network services, including those to rooms in Halls of Residence and prevent access to the facilities without notice while investigations proceed.

5.2. Cases of misuse or abuse should be reported to, and will be taken up in the first instance by the appropriate authority shown below.

Misuse by:	Report in the first instance to:
Students using centrally managed IT facilities	Director of ISD
Students using locally managed departmental facilities	Head of Department or local computer manager
Staff	Head of Department, Dean or Vice-Provost as appropriate
Anyone not included in the categories above	Director of ISD

5.3. The relevant UCL authority where appropriate, may be informed and will deal with the incident under the appropriate disciplinary procedures for students and staff. In some cases, legal action may be taken, and law enforcement informed. UCL reserves the right to disclose data or information about an individual's use of UCL's computing facilities to any appropriate or authorized third party (including law enforcement) to assist in any further investigation.

5.4. If websites containing material that may be illegal are discovered, particularly material relating to children or the exploitation of children, UCL encourages its staff and students to make a report to the authorities named above or to the Internet Watch Foundation (IWF) hotline (***http://www.iwf.org.uk***). The normal course of events is that the IWF will request that the Internet Service Providers (ISPs) in the UK will block that site. If this does not happen the IWF will inform the Police who may investigate the matter further.

5.5. Actual or suspected security violations should be reported immediately to the UCL Information Security Group (*e-mail*: ***isg@ucl.ac.uk*** or telephone 020 7679 7338 / extension 37338 within UCL). No attempt should be made to investigate security vulnerabilities unless or until appropriate authority has been obtained.

6. Further Information

6.1. Status of this document

This document has been approved by UCL's Information Risk Governance Committee.

The enrolment form signed by students explicitly binds them to abide by UCL Regulations, of which this document forms a part. UCL staff are also obliged to abide by these regulations as a condition of employment. Users of IT services who are neither staff nor students are required to complete a registration form which binds them to abide by these regulations.

In all cases the act of registering as a user of the Information Systems facilities or making use of any of the IT facilities implies acceptance of conditions of use and compliance with regulations, relevant Acts of Parliament and European Union law and directives.

From time-to-time UCL may issue good practice guidelines and reserves the right to withdraw network services to systems or services that are not operated in accordance with those guidelines.

6.2. UCL policy on connecting equipment to the UCL network

Additional regulations covering the connecting of equipment to the UCL network are given in the following document:
https://www.ucl.ac.uk/informationsecurity/policy/policy/public-policy/Monitoring

6.3. Location of this document

This document is subject to regular review by the UCL Information Risk Governance Group. For the most recent version please see: ***https://www.ucl.ac.uk/informationsecurity/policy/public-policy/computing-regulations***

Comments or questions about these regulations should be addressed to the ISD Service Desk in the first instance.

Approvals

Approved by the Information Services Governance Committee	**24-Feb-2016**
Endorsed by the Security Working Group	**5-Dec-2016**
Endorsed by the Information Risk Management Group	**14-Dec-2016**
Approved by the Information Risk Governance Group	**18-Jan-2017**
Approved by the Information Risk Governance Committee	**29-Nov-2021**