University of Liverpool

Regulations for the use of IT facilities

Reference Number	CSD-001
Title	Regulations for the use of IT facilities at the University of Liverpool
Version Number	2.1
Document Status	Active | Under Review
Document Classification	Public
Effective Date	06 March 2012
Review Date	11 August 2017
Author	John Cartwright, Chris Wooff, Steve Aldridge, Sue Byrne
Approved by	Corporate Services & Facilities Committee 06 March 2012
Implemented by	Director of Computing Services
Monitoring of compliance	Faculty Information Security Managers
Comments	11/12/2015 – section 10 (Schedule) update in accordance to addition of new legislation. 11/08/2017 – under review

REGULATIONS FOR THE USE OF IT FACILITIES AT THE UNIVERSITY OF LIVERPOOL

All individuals using IT facilities defined in these regulations must ensure that they comply with these regulations.

1. Scope

   These Regulations apply to the use of all computer, electronic information and communication facilities at or operated wholly or partly by the University of Liverpool ("the University") including:
   a. All local computing facilities, multi-user systems, server systems, work stations, personal computers, micro computers and networks or other electronic information and communication systems whether provided by the University or otherwise and which are intended wholly or partly for use by employees of, researchers or students of the University or wholly or partly for use for other University or University related or academic purposes;
   b. All remote facilities that are accessed through the computer, electronic information and communication facilities at or operated wholly or partly by the University.

2. Definitions

   The following words and phrases shall have the following meanings in these regulations:

   "Appropriate Authority"

   an individual or a group of individuals under whose control a System is placed;

   "Conditions Of Use"

   additional conditions attached to the use of a particular System by the Appropriate Authority: such conditions are subservient to these Regulations;

   "Director"

   the Director of the Computing Services Department;

   "Registrar"

   the University Registrar or Chief Operating Officer;

   "Regulations"

   these Regulations for the Use of IT Facilities at the University;

   "System"

   a system or facility which is within the scope of these Regulations as described under Scope above;

   "User"

   any person or persons granted authority to use a System or Systems whether such authority is granted to them individually or by reason of their being a member or part of a group which is authorised to use a System. Authority will only be granted to

a person or group where that person or group agrees to be bound by these Regulations;

"User Name"

a form of identifier which is given to a User by the Appropriate Authority which, together with a personal password of the User, is used to identify and authenticate the User when accessing a System.

3. Authority to use a System or System
    1. Each System will be under the control of an Appropriate Authority.
    2. The Appropriate Authority of a System has the power to allocate Users of that System, to refuse any request or application to use that System and to set out the Conditions of Use of that System by a User.
    3. The conditions of use will include the Appropriate Authority issuing a User Name to a user and will require the User to adopt a personal password for the purposes of identifying and authenticating the User when accessing a System.
    4. For certain publicly accessible Systems (such as the University's web site or on-line Library Catalogue), persons making use of these Systems will be automatically granted authority to use such Systems and hence become Users within the context of these regulations even though no User Name or personal password will be issued to access such Systems.
    5. The Appropriate Authority may at any time add to, delete or amend, as it sees fit, any Conditions of Use applicable to any User.
    6. Any authority granted to a User to use a System is limited to the User to whom authority has been granted, in particular:
        a. Authority given to a User may not be extended or transferred to any other person or persons;
        b. The User may not allow any other person (whether a User or otherwise) to access a System by way of his/her personal User Name and personal password. A User is required to keep and maintain as secret his/her personal password;
        c. A User must not use or access a System beyond that limit for which authority has been granted to that User;
        d. A User must not access a System and leave it unattended and make it available to another person.

4. Usage
    1. Systems are provided to conduct the University's business (this includes teaching, learning support, research, marketing, and other related support activities). Incidental and occasional personal usage is permitted so long as such use does not disrupt or distract from conducting University business or prevent others from carrying out University business.
    2. All Users will comply with any Policies and Codes of Practice for Use of IT at the University of Liverpool approved and issued by the University and identified in the Schedule to these regulations.
    3. All Users of all Systems will:
        a. Use the System in compliance with the Laws of England. English legislation that has been shown to be relevant to the use of Information and Communication Technology based systems is listed in the Schedule of these Regulations;

b. Adhere to the terms and conditions of all licence agreements relating to the Systems which they use including software, equipment, services, documentation and other goods;
c. Have a primary responsibility for the security and back-up of their work and data;
d. Exercise due care and consideration for the interests of the University and other Users, including the efficient use of consumables and other resources.

4. No User or person shall, knowingly or negligently:
    a. Use or access a System for any illegal or unauthorised purpose;
    b. Store or make publicly accessible any data, text, image or programme which is unlawful or, whether lawful or not, could bring the University into disrepute or does not accord with the aims or objectives of the University;
    c. Store or make publicly accessible any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into offensive, obscene or indecent images or material. For properly supervised and lawful research purposes a User may request permission to have this clause of the regulations waived. Such an application must be considered by the Registrar in advance of any potential breach.
    d. Attempt to reverse-engineer any part of a System (including software) without the written permission of the copyright owner;
    e. Create, store, process or transmit any defamatory material or material which is designed or likely to cause annoyance, harassment, inconvenience or needless anxiety to another.
    f. Store, process or distribute material that infringes the copyright of another person or organisation.
    g. If any of your activities involve the use of facilities outside the University, for example, the sending of e-mail to users at another University, you must also observe the terms of the JANET Acceptable Use policy: http://www.ja.net/company/policies/aup.html.

5. Usage Monitoring
    1. The Appropriate Authority may from time to time monitor the usage of any System under their control. This monitoring may include the monitoring of electronic communications and access to external electronic resources (e-mail and web pages).
    2. The reasons for undertaking such monitoring include: ensuring the effective operation of the system, investigating or detecting the unauthorised use of the systems, preventing or detecting crime, determining whether or not the usage is relevant to the University's business.
    3. This monitoring is permitted within the terms allowed by the Regulation of Investigatory Powers Act (RIP) 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These Regulations constitute formal notice that communications may be intercepted for reasons allowed within these Acts.

6. Commercial Usage
    1. If any work is to involve commercial usage of a System, this fact must be notified to the Appropriate Authority before any use is made of the facilities for such work. Whether or not the individual(s) concerned are authorised to use these facilities for educational purposes, further authorisation is required before commercial usage can commence, and an appropriate rate of charges must be agreed by the Appropriate Authority.

2. Where a System is to be used in connection with research grants, short courses or contracts involving specific provision for computing costs, this fact must be communicated to the Appropriate Authority and a rate of charges must be agreed before such utilisation may commence.
3. Commercial usage of software supplied under educational use only agreements is permitted only if explicit written approval has been obtained from the supplier of the software.

7. Confidentiality
    1. The University will endeavour, through its Appropriate Authorities, to take steps to protect information stored on or by means of a System. However the University will not be responsible for upholding any special restriction or condition on the handling or usage of any information unless it has been informed of the existence of such restriction or condition and has agreed to enforce it.
    2. A User processing personal data must ensure that they comply with their obligations under the Data Protection Act 1998 and the University's Data Protection Policy. The University maintains a general registration / notification under the Data Protection Act that should cover most of data used for academic purposes. Should any User be in any doubt about their obligations under the Data Protection Act they should consult the University Data Protection Officer.

8. Breach of the Regulations
    1. The Registrar has power to withdraw (either temporarily or permanently) the authority of any User to use any System in circumstances where the Registrar reasonably believes a User has breached these Regulations.
    2. The Registrar may temporarily suspend the authority of any User of any System where the Registrar suspects that a User may have breached these Regulations, pending an investigation into the suspected breaches.
    3. A breach of these Regulations may also constitute a criminal or civil offence, for example under the Computer Misuse Act 1990, the Telecommunications Act 1984, and the Obscene Publications Acts 1994. A breach of these Regulations may also be a breach of the Copyright Laws. In the event that the Registrar suspects that a User may have committed an offence, the police or other appropriate enforcement authority may be contacted to investigate whether an offence has been committed.
    4. The Director has the same powers as the Registrar as set out in clauses 1, 2 and 3 above in connection with any System for which either the Director or the Computing Services Department is the Appropriate Authority. The Director will inform the Registrar of any decisions taken with respect to clauses 1,2 and 3.
    5. In addition to the possible sanctions in these Regulations, a suspected breach of these Regulations may also be investigated in accordance with the University's internal disciplinary procedures. A significant breach of these Regulations may be regarded as gross or serious misconduct.
    6. A User who is in breach of these Regulations, (whether directly or by giving unauthorised permission to someone not registered or another User to use a System) will indemnify and hold harmless the University against all costs incurred by and losses caused to the University by reason of such breach, including (but not limited to) repair costs, any claim for damages, legal costs, fines or other financial penalties.

9. Disclaimer

   The University undertakes to provide and operate Systems with reasonable care and skill, but accepts no liability for any loss or damage a User may suffer from any failure or malfunction of a System.

10. Schedule

    1. English and International Laws that have been found to be relevant to the usage of Systems include:

       a. Obscene Publications Act 1959 and 1964
       b. Protection of Children Act 1978
       c. Police and Criminal Evidence Act 1984
       d. Copyright, Designs and Patents Act 1988
       e. Criminal Justice and Immigration Act 2008
       f. Computer Misuse Act 1990
       g. Human Rights Act 1998
       h. Data Protection Act 1998
       i. Regulation of Investigatory Powers Act 2000
       j. Data Retention Investigatory Powers Act 2014
       k. Counter Terrorism and Security Act 2015, inc statutory guidance (Prevent), section 26, schedule 6
       l. Police and Justice Act 2006
       m. Freedom of Information Act 2000
       n. Freedom of Information (Scotland) Act 2002
       o. Equality Act 2010
       p. Privacy and Electronic Communications (EC Directive) Regulations 2003
       q. Defamation Act 1996 and 2013
       r. Protection from Harassment Act 1997
       s. Communications Act 2003

    2. Policies for the Use of IT Facilities at the University include:
       a. Summary of the Regulations for the Use of IT Facilities at the University of Liverpool
       b. Information Security Policy
       c. Card Payment Policy
       d. Information Asset Classification Policy
       e. Information Security Incident Response Policy
       f. Information Security Review Policy
       g. IT Asset Disposal Policy
       h. IT Procurement and Third Party Security Policy
       i. Research Data Management Policy
       j. Security Investigation Policy
       k. Social Media Compliance Policy
       l. Testing Policy and Strategy
       m. Workspace and IT Equipment Security Policy

    3. Codes of Practice for the Use of IT facilities at the University include:

       a. Code of Practice for Using Cloud Services