University of Salford
A Greater Manchester University

# Acceptable use of ICT Facilities Policy

## Contents


**Document Control Information** ..... 1
**1.0 Introduction** ..... 2
**2.0 Purpose** ..... 2
**3.0 Scope** ..... 2
**4.0 Responsible Authorities** ..... 2
**5.0 Policy Statements** ..... 2
5.1 General ..... 2
5.2 Acceptable Use ..... 3
5.3 Personal Use ..... 3
5.4 Unacceptable Use ..... 4
5.5 Prevention, Detection & Investigation of Misuse ..... 5
**6.0 Legislation** ..... 6
6.1 Computer Misuse Act 1990 ..... 6
6.2 Data Protection Act 1998 ..... 6
6.3 Libel ..... 6
6.4 Copyright ..... 7
**7.0 Sanctions** ..... 7
**8.0 Other References** ..... 7


## Document Control Information

| | | | |
|---|---|---|---|
| **Document Ref:** | ICT AUP | **Version:** | 1.0 |
| **Classification:** | Unrestricted | **Status:** | Issued |
| **Effective from:** | July 2005 | **Review Date:** | July 2006 |
| **Originated by:** | Q&P Unit , ISD | **Date:** | 07/04/05 |
| **Approved by:** | Personnel Committee, Senate, Council | **Date:** | 29/06/05 |
| **Authorised by:** | Personnel Committee, Senate, Council | **Date:** | 29/06/05 |
| **Issued by:** | Director, ISD | **Date:** | 15/07/05 |
| **Change History:** | This policy statement replaces in its entirety the previous statement | **Date:** | 15/07/05 |
| **Change Forecast:** | Further changes are expected at each annual review, and more frequently if new security threats demand new measures | **Date:** | |
| **Circulation:** | | All University staff & students via the University intranet | The general public via the University web site |

| | |
|---|---|
| **Enquiry point :** | IT Security Co-ordinator<br>University of Salford<br>Information Services Division<br>Clifford Whitworth Building<br>SALFORD<br>M5 4WT<br>Std: 0161 295 5910<br>Mobile:<br>Fax: |

## 1. Introduction

This document defines the University of Salford's policy in respect of the acceptable use of its information and communications technology (ICT) facilities.

## 2. Purpose

ISD is responsible, on behalf of the University, for minimising and containing potential risks to the University and its members, both operational and legal, from the consequences of the misuse of its ICT facilities. The purpose of this policy is therefore to state clearly both users' obligations in using these facilities and ISD's responsibility and authority in taking action to safeguard them.

## 3. Scope

This policy applies to all staff, students, contractors, consultants, authorised guests and other personnel at the University of Salford and includes Acceptable Use, Personal Use and Prohibited Use of the University's ICT facilities, which encompass (but are not restricted to):

- network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers
- network services, including (but not exclusively) internet access, web services, email , wireless, messaging, telephony and fax services
- computing hardware, both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, PDAs, servers, printers, scanners, disc drives, monitors, keyboards, tablets and pointing devices
- software and databases, including (but not exclusively) applications and information systems, virtual learning and videoconferencing environments, language laboratories, software tools, information services, electronic journals & ebooks

## 4. Responsible Authorities

The term **"Designated ISD Authority "** used in this policy means the Director of Information Services or his / her authorised delegate. This policy is issued under the authority of the Director of Information Services who as an Officer of the University is responsible for enforcing sanctions where necessary to safeguard the University and its members. The IT Infrastructure is managed by the Head of IT Infrastructure and Operations who is responsible for the prevention and detection of ICT misuse. This policy is managed by the Head of Quality & Processes who is responsible for investigating incidents of ICT misuse.

## 5. Policy Statements

### 5.1 General

It is the policy of the University:

- to provide a working environment that encourages access to knowledge and sharing of information
- to maintain ICT facilities for academic and administrative purposes which provide access to its community for local, national and international sources of information

- that ICT facilities will be used by members of its community with respect for the public trust through which they have been provided, and in accordance with prevailing laws and such regulations and policies established from time to time by the University and its Senate, Faculties, Boards and other bodies.
- To ensure that the University is protected by holding users responsible for safeguarding passwords and access identities. Passwords and identities must not be shared.

### 5.2 Acceptable Use

It is the policy of the University:

- that the University's ICT facilities are provided in support of the University's teaching, learning, research, enterprise, and administrative activities
- that they may be used for any purpose that is in accordance with the aims and policies of the University (as defined in the ISD regulations) and the JANET Acceptable Use Policy, including interworking with other organisations e.g. Net North West.
- that only registered users (i.e. those holding valid ISD usernames and passwords) or those given permission by the designated authority are permitted to use the University's ICT facilities.
- that users are expected to:
    - be prepared to show ISD staff their ID card as proof of identity. This must be shown when requesting any changes to a network account.
    - respect the published times of access to the facilities
    - respect the rights of others, and conduct themselves in a quiet orderly manner when using the open access facilities
    - comply with all valid regulations and legislation covering the use of Copyright and licensed material, including software, whether those regulations are made by law, or the originator of the material, or the distributor of the material (e.g. CHEST), or the University, or by any other legitimate authority
    - make all reasonable efforts to send data that is 'Virus Free', and to protect themselves from viruses and hacking attempts when connected to the University's network either on or off Campus. The University will not be held responsible for any damage to users' systems or information that occurs through such virus or hacking attacks.
    - conform to all other appropriate policies and guidelines from ISD (including netiquette guidelines), the University (including web page design guidelines), and externally (including the JANET Acceptable Use Policy).

### 5.3 Personal Use

The University accepts that a member's Personal Use of the University's ICT facilities is within the scope of Acceptable Use, subject to the provisos within this document. It is the policy of the University:

- that provided that personal use is occasional and reasonable and does not interfere with , nor detract from an individual's everyday workload and commitments, nor with the effective functioning of the University or any part of it, and that it complies with all other terms of this Acceptable Use Policy then it will normally be tolerated
- to reserve the right to withdraw access to ICT facilities for this category of use at any time.

### 5.4 Unacceptable Use

It is the policy of the University to prohibit the use of its ICT facilities when used or attempted to be used intentionally in contravention of the general principles outlined in 5.1 above. The activities prohibited under this policy include (but are not restricted to) those listed below. Users must not:

i. cause the good name & reputation of the University or any part of it to be damaged or undermined;

ii. create or transmit (other than in the course of properly supervised academic research where this aspect of the research has the explicit approval of the University's official processes for dealing with academic ethical issues) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

iii. access, create, change, store, download or transmit material which the University may deem to be threatening, defamatory, abusive, indecent, obscene, racist or otherwise offensive;

iv. place links to websites which have links to, or displays pornographic and inappropriate material, facilitate illegal or improper use, or to bulletin board which are likely to publish defamatory materials or discriminatory statements; or where copyright protected works such as computer software or music are unlawfully distributed ;

v. generate excessive noise, cause annoyance, inconvenience or needless anxiety to, or to violate the privacy of, anyone else;

vi. allow the ICT facilities to be damaged or contaminated by food, drink or smoking materials;

vii. interfere with the legitimate use by others of the ICT facilities, or interfere with or remove computer printout or media belonging to others;

viii. send unwanted, e-mail, chain letters, hoax virus warnings, pyramid letters or similar schemes using the University e-mail system;

ix. falsify E-mails to make them appear to have been originated from someone else;

x. make use and possess, distribute, sell, hire or otherwise deal with any unauthorised copies of computer software for any purpose without the license of its owner;

xi. install any software that is not licensed to the University and /or install without authorisation software licensed to the University on any of the University's computer systems under any circumstances;

xii. transmit unsolicited unauthorised commercial or advertising material;

xiii. use the ICT facilities for commercial , social or group distribution activities unless permission has been formally granted by the Designated ISD Authority;

xiv. gain unauthorised personal commercial benefit;

xv. gain unauthorised access to facilities or services via the University network;

xvi. allow others to gain such unauthorised access, either wilfully by disclosing user names or passwords or neglectfully by failing to log out of the system, thereby permitting unauthorised use of a University account;

xvii. disseminate any material which may incite or encourage others to carry out unauthorised access to or unauthorised modification of the University's or others' computer facilities or materials;

xviii. introduce and transmit material (including, but not restricted to, computer viruses, Trojan horses and worms) designed to be destructive to the correct functioning of computer systems, software, networks and data storage, or attempt to circumvent any precautions taken or prescribed to prevent this;

xix. attempt to circumvent the University's firewall systems, or use file-sharing systems (sometimes known as P2P or peer-to-peer) without first gaining the permission of the designated authority;

xx. change, damage, dismantle, corrupt, or destroy (or cause to be changed, damaged, dismantled, corrupted or destroyed) any network component, equipment, software or data, or its functions or settings, which is the property of the University, its partners, staff, students, visitors, or anyone else, without the express permission of the designated ISD authority;

xxi. cause any of the University's ICT services to be overloaded, impaired, disrupted, curtailed or denied (other than in compliance with the direct instruction of the designated ISD authority);

xxii. connect any non approved computer network equipment (including wireless access points) to the University network without first gaining the written permission of the Designated ISD Authority (this excludes normal and reasonable use of computer equipment connected to network points in student rooms within University halls of residence);

xxiii. set up any network services (eg web servers, e-mail services etc) unless formally sanctioned by the designated ISD authority;

xiv. register any domain name which includes the name of the University or any name which may mislead the public into believing that the domain name refers to the University;

xxv. use equipment (including mains leads) which has not first been PAT Safety tested (Portable Application Tested) by University approved staff; the equipment must display an up to date PAT label;

xvi. continue to use any item of networked hardware or software after a designated ISD authority has requested that use ceases because of its causing disruption to the correct functioning of the University ICT facilities, or for any other instance of Unacceptable Use;

xxvii. fail to comply with any action directed by a designated ISD authority to prevent or respond to any threats to the correct functioning of the University ICT facilities;

xviii. contravene the local rules for University ICT facilities outside ISD;

xix. create or transmit material that infringes the copyright of another person or institution, or infringe the Copyright laws of the UK and other countries;

xxx. interfere with the legitimate activities of other users covered within the principles outlined in Section 5.2 of Acceptable Use;

xxi. otherwise act against the aims and purposes of the University as specified in its rules, regulations, policies, and procedures adopted from time to time

xxii. contravene applicable laws and prevailing regulations and policies applied by bodies external to the University, including but not restricted to JANET (the Joint Academic Network).

### 5.5 Prevention, Detection & Investigation of Misuse

Monitoring may take place periodically within the guidelines set down by the Regulation of Investigatory Powers Act (RIPA) 2000.

The University retains the right under the RIPA Act to access all information held on its information and communications facilities to monitor or intercept any system logs, web pages, E-mail messages, network account or any other data on any computers system owned by the University. This will be for the purposes of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and University policies, or to secure effective system operation.

The University reserves the right to inspect and validate any items of University owned computer equipment connected to the network. Any other computer equipment connected to the University's network can be removed if it is deemed to be interfering with the operation of the network.

It is the policy of the University:

- to publish its Acceptable Use Policy and to promote this to all users of the University Network
- to provide advice to staff and students, on request, on matters relating to acceptable use
- to take swift and effective action within existing disciplinary and / or legislative frameworks against anyone found to be intentionally misusing the information and communications facilities.

In all cases where there is the potential for the University's ICT facilities to be misused, it is the University's policy to:

- record the identity of the individual using the specific facility at any given time
- retain these records for not less than three calendar months, and shall make them available to those senior managers appointed by the University to investigate complaints of misuse
- destroy these records after twelve calendar months unless required in connection with a specific investigation.

## 6. Legislation

### 6.1 Computer Misuse Act 1990

It is a criminal offence (Computer Misuse Act 1990) to gain unauthorised access to a computer system to make any unauthorised modification of computer material (including the introduction of a computer virus) or to interfere with any computing system provided in the interests of health and safety. For more information see http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

### 6.2 Data Protection Act 1998

The Data Protection Act 1998 regulates the storage of personal information (i.e. any information that can be identified as relating to a particular person or person(s) on computer systems. Before storing any such information on the University computer system, you must notify the University Data Protection Officer in writing. It is everyone's responsibility to ensure that any such information complies with the law. For more information regarding Data Protection see http://www.dataprotection.gov.uk

### 6.3 Libel

Libel is a civil wrong, which in proven cases, may incur substantial compensation. It is very complicated and therefore one of the easiest laws to contravene through ignorance. Facts concerning individuals or organisations must be accurate, verifiable and views or opinions must not portray their subjects in any way that could damage their reputation. Check with the University Legal Office before publicly displaying any contentious material. Web pages and E-mail messages are regarded as published material.

### 6.4 Copyright

The Copyright laws of the UK and other countries must not be infringed. Downloading material from the Internet carries the risk of infringing copyright. This applies to files, music, films, TV programmes, documents and software , which must be licensed. Material illegally copied in this country or elsewhere and then transmitted to another country via the Internet, will also infringe the copyright laws of the country receiving it.

Copyright, Design and Patents Act 1998 is applicable to all types of creations, including text, graphics and sounds by an author or artist. This will include any that are accessible through the University's computer systems.

Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of her/his rights.

Users must not make, transmit or store an electronic copy of copyright material on the University's computing services without the permission of the owner. For more information see: http://www.isd.salford.ac.uk/publica/notes/copyright.pdf

For more information regarding the 'Legal Framework' which consists of a schedule of the laws with which we must comply is detailed at: ……

## 7. Sanctions

Where misuse of ICT facilities has been identified, the matter will be investigated under the University's appropriate disciplinary procedure. As an officer of the University, the Director of Information Services or his / her nominee has the authority to investigate cases of alleged misuse and where applicable to apply sanctions directly, or to refer individuals to their faculty / school / division for disciplinary action.

Any misuse which is in contravention of the law and/or which involves the intentional access, creation, storage or transmission of material which may be considered indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the University's official processes for dealing with academic ethical issues) will be regarded as an act of gross misconduct.

Students may be expelled for gross misconduct under the University's student disciplinary procedures and staff may be dismissed under the University's staff disciplinary procedures.

Where there is evidence of a criminal offence, the issue will be reported to the Police for them to take action. The University will co-operate with the Police and other appropriate external agencies in the investigation of alleged offences.

## 8. Other References

Users are bound by the Law of England and Wales when using the University's ICT facilities e.g. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 at:

http://www.hmso.gov.uk/si/si2000/20002699.htm

In addition, when accessing computers abroad, the rules of that country apply.

It is the user's responsibility to ensure his/her activities comply with these laws.

The use of the University's information systems facilities is subject to all relevant University regulations detailed at : http://www.salford.ac.uk/policies_procedures

The use of some information systems software is subject to the Chest Code of Conduct detailed at: http://www.chest.ac.uk/conduct.html .

When making use of the Internet, the acceptable use policies of the carriers apply, in particular those of Net North West and JANET http://www.ja.net/services/publications/policy/aup.pdf.

When developing externally-visible websites, reference must be made to the University's web publishing guidelines at: http://intranet.salford.ac.uk/extrel/webteam/documents/web_publishing_guidelines_2004-v6.doc.

Users of the University's email services should follow the E-mail etiquette guidelines for using e-mail effectively, securely, considerately and legally, available at:

http://www.isd.salford.ac.uk/publica/notes/emailetiq.pdf