

USE OF UNIVERSITY COMPUTERS AND DATA NETWORKS

University Policy

It is the policy of the University to encourage the proper use of its computing and networking facilities in support of its teaching, learning, scholarship and research activities. In pursuance of this policy the University will promote good practice guidelines and implement and publicise procedures for enabling it to comply with the provisions of the relevant legal acts and with the conditions of the JANET Acceptable Use Policy. (JANET is the UK's Joint Academic Network, to which the University's network is connected.)

Rules

The following rules apply to any person using any kind of computer hardware or software, for any purpose, at the University, including the use of personal equipment on University premises and remote use of the University's network.

1. Users

- 1.1 All users of the University's IT facilities must be registered with IT Services. All users will be registered staff or student members of the University. Use of the facilities by non-members of the University may be arranged in certain cases and may be subject to charge.
- 1.2 Registration to use IT facilities or the use of IT facilities constitutes acceptance of these Rules and Regulations.
- 1.3 Users are responsible for all use of the computer logon account allocated to them, defined by an identifier (username or logon name) and password. They must not use another user's identifier or password nor allow any identifier or password issued to them to become known to any other person.
- 1.4 The University's IT facilities are for bona fide University activities. Permission must be sought via the Head of IT to use the facilities for commercial or outside work and such use may be subject to charge. Use of the facilities for personal work or recreation will only be permitted within reasonable levels and must not jeopardise or interfere with the system so as to reduce the level of service for University business.

2. Law

- 2.1 It is the user's responsibility to comply with all statutory and other provisions and regulations currently in force in the field of data protection and information policy.
- 2.2 Laws applicable to the use of the University's IT facilities include:
 - a) Data Protection Act 1998
 - b) Copyright, Designs and Patents Act 1988
 - c) Computer Misuse Act 1990
 - d) Criminal Justice and Public Order Act 1994.

Users must comply with the provisions of the above acts and particular attention is drawn to the following:

Under the Computer Misuse Act, hacking and the introduction of viruses are criminal offences. The Act identifies three specific offences:

- Unauthorised access to computer material (i.e. a program or data)
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime
- Unauthorised modification of computer material.

All three offences are punishable by fine or imprisonment or both.

- 2.3 The University's rules for the use of IT facilities apply subject to and in addition to the law. In all cases involving a breach of the law legal sanctions may apply.

3. Use of Software and Data Networks

- 3.1 Users must adhere to the conditions laid down by the JANET Acceptable Use Policy. Copies of the Policy are available from the IT Services helpdesk and are displayed in student computer rooms and on the University Web site.
- 3.2 Users must not access, or try to access, any computer material or system for which access authorisation has not been given.
- 3.3 The creation, display, production or circulation (other than for properly supervised and lawful research purposes) of offensive, obscene or indecent material in any form or medium is forbidden.
- 3.4 Users must adhere to the terms and conditions of all licence agreements relating to software and data networks.
- 3.5 Users are required to respect the copyright of all materials and software made available by the University's IT facilities. The unauthorised copying or modification of software is an offence under the Copyright, Designs and Patents Act 1988.
- 3.6 Users must not load onto the IT facilities any software without permission from IT Services. IT Services shall maintain a register of authorised software installed on University computers and shall have the right to remove without notice any software not so registered.
- 3.7 Users must not deliberately introduce, or risk introducing, any virus or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any anti-virus precautions established by IT Services.
- 3.8 Users must not construct or maintain computer files containing data about living individuals without complying with the principles of the Data Protection Act. Advice on the requirements of the Act can be obtained from the Data Protection Officer.
- 3.9 Users must not use the system or networks in a way that denies service to other users (for example, deliberate or reckless overloading).
- 3.10 Users' data and software will be subject to published procedures for their removal and archiving after specified periods.
- 3.11 Users of networks and remote IT facilities shall obey any published rules for their use.
- 3.12 Users must not in any way cause any form of damage to the University's IT facilities, nor to any of the accommodation or services associated with them.

4. Use of Equipment and Computer Rooms

- 4.1 Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use to make their use of it safe and effective and to avoid interference with the use of it by others.
- 4.2 Users must take every precaution to avoid damage to equipment caused by smoking, eating or drinking in its vicinity. In particular, smoking, eating or drinking in any student computer room is forbidden.
- 4.3 Users must not transfer within or remove from University premises any item of computer hardware (including peripheral devices such as printers) without written permission from IT Services.
- 4.4 No equipment may be connected in any way into any University network without the prior written agreement of IT Services.
- 4.5 Users must not interfere with the use by others of the IT facilities; they must not remove or interfere with output belonging to another user.
- 4.6 Users shall adhere to any procedures pertaining to the security of IT facilities. In particular:
 - a) Access to student computer rooms must be by uCard only, doors must not be propped open;
 - b) uCards are the responsibility of the assigned user and must not be used by any other person.

5. Disclaimer of Liability

- 5.1 Whilst IT Services takes appropriate security measures to protect data and software, the

University cannot and does not accept any responsibility for the loss of any data or software or the failure of any security or privacy mechanism.

- 5.2 The University accepts no responsibility for the financial or other consequences of the malfunctioning of any IT facility or part thereof, whether hardware, software or other.
- 5.3 No claim shall be made against the University, its employees or agents in respect of any loss, damage or inconvenience alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

6. Failure to Observe the Rules

- 6.1 Any infringement of these Rules may be subject to penalties under civil or criminal law and the University is prepared to invoke such law.
- 6.2 Any infringement of these Rules constitutes a disciplinary offence and, regardless of legal proceedings, established disciplinary procedures will be followed for staff and students.
- 6.3 For the general guidance of students, the least serious offences are liable to result in temporary withdrawal of facilities and a formal warning. More serious offences will carry longer terms of suspension and possibly fines, together with a formal warning. In the most serious offences termination of studies will be considered.
- 6.4 Authority is vested in the Head of IT and Officers of the University temporarily to suspend access to IT facilities by any user suspected of a breach of these Rules pending full investigation.

EMAIL POLICY

1 The Policy

- 1.1 The purpose of this Policy is to provide information about the provision of the University's email services and to provide guidelines for users to help ensure effective, safe, and responsible use.
- 1.2 The Policy applies to all University staff and students and to any other authorised user.
- 1.3 The Head of IT Services is responsible for drafting the Policy, directing it through the consultative and approval processes and for periodically reviewing it.
- 1.4 Email services are part of the University's overall IT provision and this Policy should therefore be read in conjunction with the following related documents:
 - 1.4.1 Rules and Regulations on the Use of University Computers and Data Networks.
 - 1.4.2 The JANET Acceptable Use Policy.
- 1.5 The Policy will be distributed to all users and made available on the University Web site.

2 Principles of Email Provision

- 2.1 The University provides email facilities to authorised users for the purposes of teaching, learning, research, administration and approved business activities. Limited personal use is allowed under certain conditions (specified in 7.4 below).
- 2.2 All email use is subject to:
 - 2.2.1 The relevant legislation.
 - 2.2.2 The University's Rules and Regulations on the Use of University Computers and Data Networks.
 - 2.2.3 The conditions of the JANET (Joint Academic Network) Acceptable Use Policy.
 - 2.2.4 The conditions and guidelines established in this Email Policy.
- 2.3 Email cannot be assumed to be a secure medium and should not be used for the transmission and/or storage of confidential data.

3 Statement of Responsibilities

- 3.1 The Head of IT Services is responsible for developing and communicating policies and procedures for the University's email system and its usage. The Head of IT Services is also responsible for dealing with complaints regarding email usage and, in the first instance, for dealing with breaches of the conditions of this Policy.