

Finance & IT Directorate

IT Conditions of Use

All facilities are provided to members of the university on acceptance and use of a Keele University Username and Password.

1 Terms used

- 1.1 Reference throughout the document is made to
- Members of the University include staff, students, visiting authorised users
 - University – Keele University
 - User – includes staff, student, visiting authorised users
 - Director – Director of Finance & IT or designated officer.
 - JANET – Joint Academic Network
 - IT systems – communication, telephones, network facilities, hardware, software
 - Username - IT Account Name
- 1.2 In abiding by the terms of these conditions your attention is drawn to the following additional policies that are incorporated within:-
- Chest Code of Conduct - <http://www.eduserv.org.uk/chest/conduct.html>
 - Janet Acceptable Use Policy - <http://www.ja.net/services/publications/policy/aup.pdf>
 - Keele University Policy on Monitoring and Interception of IT Systems – <http://www.keele.ac.uk/depts/cc/policy/>
 - Guidance & University Policy on Data protection - http://www.keele.ac.uk/admin/ps/governance/Data_protection/dpa_home.htm

2 Service Provision

- 2.1 Keele University IT systems are provided for members of the University to support the University's mission.
- 2.2 Keele University's network connects to JANET, the private network for the UK's education and research community. The purpose of JANET is to support research and education among the academic community.
- 2.3 The Finance and IT Directorate has executive responsibility for all Information Technology and Information Systems at the University including links to the Internet.
- 2.4 The IT systems may be used for any legal activity that is in furtherance of the aims and policies of the University.
- 2.5 These conditions apply to members of the University and other authorised persons, who are authorised by the Director to use University IT Systems, Networks and Datasets.
- 2.6 Authorisation will be granted to all members of the University and a non-transferable username and password will be issued to enable access to the relevant IT Systems. The Director has the discretion to authorise other persons to use the facilities.
- 2.7 Email communication exists primarily for business purpose although personal usage is permitted. It is the primary form of communication within the University, and is expected to be accessed on a regular basis by all authorised users.
- 2.8 Registration will lapse for staff upon termination of appointment (paid or titular) and for students on completion or withdrawal from their course of study.
- 2.9 The use of University IT Systems and networks are subject to inspection by Finance & Information Technology staff for the purposes of monitoring and assessment. Further details regarding monitoring can be found in the Monitoring and Interception of IT Systems Policy (http://www.keele.ac.uk/depts/cc/documents/monitor_rip.htm).
- 2.10 Registration may be suspended or withdrawn at any time at the discretion of the Director.
- 2.11 No person may make use of IT facilities without prior authorisation from the Director.
- 2.12 The Director may at any time remove a user's files, data and/or software from University systems, whether or not the property of the University, if they are deemed to cause a reduction in the efficiency or quality of service or bring the University into disrepute.
- 2.13 The Director reserves the right to withdraw facilities from users or disconnect equipment which adversely affect IT systems.

3 Usage Conditions

3.1 *Acceptable Use*

- 3.1.1 Authorised users are those users accessing University IT systems in the pursuance of their duties, education and training.

- 3.1.2 Authorised Users must conduct themselves honestly, respecting other users, observing copyright rules, software licensing rules, property rights and privacy of others. All existing University policies and Legislation (Section 6) apply to users conduct whilst using the IT systems, especially harassment, misuse of resources, information and data security and confidentiality.
- 3.1.3 Users may access external IT systems from the University. They must abide by the regulations governing the use of these external facilities. In particular users of the JANET network are subject to the JANET Acceptable Use Policy. (<http://www.ja.net/documents/publications/policy/aup.pdf>).
- 3.1.4 All software applications provided by the University must be used in accordance with the CHEST Code of Conduct¹ (<http://www.eduserv.co.uk/licence-negotiation/general/conduct.aspx>) and its associated Copyright Acknowledgement (<http://www.eduserv.co.uk/chest/appendix-b.aspx>).
- 3.1.5 Users are permitted to connect approved personal equipment to the network provided it is configured as specified by the University.
- 3.1.6 Users are permitted reasonable personal use.

3.2 *Unacceptable Use*

IT systems must not be used for the following:

- 3.2.1 To access, store or transmit pornographic, discriminatory, defamatory or offensive material or undertake any transmission of information that contravenes University Regulations, policies or current legislation.
- 3.2.2 Running software to provide services to other users including running a file server for use by a third party. This includes the use of filesharing or peer to peer software on University or personal equipment connected to the University network, unless authorized by the Director.
- 3.2.3 The disclosure of usernames and passwords which are intended for sole use of the member or authorised user, to gain access to university facilities.
- 3.2.4 The transmission or distribution of material such that this infringes the copyright of another person or organisation including, but not limited to, computer software, music, videos, written text or images.
- 3.2.5 Deliberate activities which cause or potentially cause loss or reduction of service to other users including but not exclusively
 - Corrupting or destroying data belonging to other users
 - Violating the privacy of other users
 - Disrupting the work of other users
 - Using systems in a way that denies service to other users
 - Introducing viruses, Trojan horses, worms or similar
 - Circumventing the effectiveness of installed security measures
 - Connecting equipment to the network that causes a deterioration of service
- 3.2.6 The transmission of unsolicited commercial or advertising material, save where that material is embedded within or is otherwise part of a service to which the user has chosen to subscribe.
- 3.2.7 Any use related to a personal business
- 3.2.8 Contract work or money-making activities not sanctioned by the University
- 3.2.9 Extending the network without prior permission from the Director.
- 3.2.10 Personal use which inhibits the use of facilities for University purposes by others or which interferes with the performance of duties, education or training.

3.3 *Due Care*

- 3.3.1 Information concerning individuals or organisations must be accurate and verifiable and views or opinions must not portray their subjects in any way which could damage their reputation.
- 3.3.2 Users should remember that any comments made in an 'open' environment reflect not only upon themselves, but also upon the University.
- 3.3.3 Access should be restricted to any material which might be considered damaging to minors. This could include, but is not limited to transcripts of research material.
- 3.3.4 Access to sensitive information should be restricted as appropriate.
- 3.3.5 All appropriate measure must be taken to ensure that University computer equipment is secure.
- 3.3.6 Users should exercise due care, not to damage or deliberately deface University computer equipment.⁽²⁾

¹ "Eduserv Chest is the software and information negotiation and licensing service for educational institutions in the UK"

² University computer equipment relates to all infrastructure, hardware and software owned/leased by the University.

- 3.3.7 All appropriate measures, as instructed by the Director, must be taken to protect data/software.
- 3.3.8 Compliance with University Data Protection Policy must be upheld by all users of IT systems.
- 3.3.9 All Users must also be aware of the implications of the Freedom of Information Act, which gives the public a general right of access to information held by the University. http://www.keele.ac.uk/admin/ps/governance/foiact/foia_home.htm

4 Breaches of conditions

Breaches of these conditions may:

- 4.1 Result in the removal of user's access to IT systems if their activities adversely affect other users.
- 4.2 Result in the withdrawal of facilities during an investigation by Finance and IT Directorate.
- 4.3 Lead to a referral to the appropriate University Disciplinary procedures⁽³⁾.
- 4.4 Where there is an alleged offence under any current UK law, it may result in criminal prosecution or civil action.

5 Charges for services

- 5.1 The University may make a charge for the use of its IT systems or related services.
- 5.2 Authorised users who incur debts for any services will be refused any IT services until these debts have been settled within the normal terms of business.

6 Compliance with Legislation

- 6.1 Within this policy members must be aware and comply with the relevant legislation and legal precedents including, but not exclusive too, the provisions of the following Acts of Parliaments or any future amendments to these acts-

- Copyright, designs and Patents Act 1988 http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm
- Malicious Communications Act 1988 http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm
- Computer Misuse Act 1990 http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
- Criminal Justice and Public Order Act 1994 http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm
- Trade Marks Act 1994 http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940026_en_1.htm
- Data Protection Act 1998 <http://www.opsi.gov.uk/acts/acts1998/19980029.htm>
- Human Rights Act 1998 <http://www.opsi.gov.uk/acts/acts1998/19980042.htm>
- Freedom of Information Act 2000 <http://www.opsi.gov.uk/acts/acts2000/20000036.htm>
- Communications Act 2003 <http://www.opsi.gov.uk/acts/acts2003/20030021.htm>
- Regulation of Investigatory Powers Act 2000 <http://www.opsi.gov.uk/Acts/acts2000/20000023.htm>
- Electronic Commerce (EC Directive) Regulations 2002 <http://www.opsi.gov.uk/si/si2002/20020213.htm>
- The Police and Justice Act 2006 Clauses 33-36
www.publications.parliament.uk/pa/cm200506/cmbills/119/2006119.pdf
- Lawful Business Practice Regulation 2000
- Obscene Publications Act 1959 & 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Employment Code of Practice 2002
- Prevention of Terrorism Act 2005
- Terrorism Act 2006

7 Liability

- 7.1 The University has no obligation to retain a User's computer files after that user's authorisation has terminated.
- 7.2 The University will not accept any liability for loss or corruption of information held, or for damages, injury to third parties, economic loss whether caused by negligence or otherwise, or expenses which may result from the use of Computing and Information Systems or withdrawal at any time of such facilities by the University.
- 7.3 The University reserves the right to take legal action against individual who cause it to be involved in legal proceedings as a result of a breach of this policy and to seek reimbursement of any consequent damages, costs or other expenditure awarded against the University or incurred by it.
- 7.4 The University accepts no responsibility for the correctness of results produced by computing systems, for the failure of the facilities to produce results, for the loss or corruption of stored information or for any consequential loss or damage.

³ To include, but not limited to, Student Regulation 20 Student discipline and Regulation 21 General Disciplinary Matters
February 2010