



Regulations for the Acceptable Use of University Information Technology (2008)

1. Interpretation

The terms listed below have within these regulations the meanings given for each.

- 1.1 University
Canterbury Christ Church University.
- 1.2 Unit
A managed organisational part of the University whether academic, administrative or other, e.g. division, department, section, faculty, unit, service, campus.
- 1.3 Staff
Staff, whether academic, administrative, technical or other employed by the University.
- 1.4 Student
An individual registered with the University or undertaking study of any kind provided by, at or under the auspices of the University. This includes pre-registered students who have not yet started their studies and students post completion of their studies for the period they are able to use University IT facilities.
- 1.5 Associate
Any person other than a member of staff or student who has an association with the University that requires access to any IT equipment or facility.
- 1.6 IT facility
Personal computers whether desktop or portable, mini or mainframe computers, servers and computer networks; all software and data thereon; all computer-based information systems provided for administrative or other purposes.
- 1.7 Damage
Any deliberate or accidental damage, or act intended to cause damage, to any IT facility or University property. This includes physical damage or any modifications to hardware, software, web pages or processes which incur time or cost in restoring the system to its original state.
- 1.8 Designated Authority
Head of Computing Services or his nominee

2 Scope

- 2.1 These regulations apply to any individual using any University IT facilities owned, leased, hired or otherwise provided by the University; any IT facilities connected directly or remotely to the University's network or IT facilities, and to any IT facilities used on the University's premises or elsewhere.

- 2.2 They apply to IT facilities in all buildings and on all campuses, in any other outlying Unit, and to IT facilities lent out by the University for use in any location.
- 2.3 The Regulations should be interpreted such that they have the widest application; in particular they include departmental systems, IT facilities owned or managed by any associated Company, and any IT facilities provided by partners or in shared facilities.

3 Legal Constraints and other Regulations

- 3.1 Applicable laws include, but are not limited to:
 - a) Health and Safety at Work etc Act (1974)
 - b) Computer Misuse Act (1990)
 - c) Defamation Act (1996)
 - d) Criminal Justice and Public Order Act (1994)
 - e) Data Protection Act (1998)
 - f) Human Rights Act (1998)
 - g) Copyright, Designs and Patents Act (1988)
 - h) Malicious Communications Act (1988)
 - i) Regulation of Investigatory Powers Act (2000)
 - j) Freedom of Information Act (2000)
 - k) Communications Act (2003)
 - l) Prevention of Terrorism Act (2005)
 - m) Terrorism Act (2006)
 - n) Police and Justice Act (2006)
 - o) The Waste Electrical and Electronic Equipment Regulations (2006)
- 3.2 These regulations apply subject to and in addition to the law. In all cases involving a breach of the law legal sanctions may apply.
- 3.3 All users of University IT facilities must comply with all other University ratified and published policies and procedures. In particular, the Information Security Policy and Procedures, the Data Protection Policy, the Email Policy and the Internet Access policy.
- 3.4 Staff Terms and Conditions of Employment, other University policies and procedures and the Staff Handbook also set out employees' responsibilities with respect to their use of computer based information systems and data.
- 3.5 The Student Regulations set out students' responsibilities regarding their use of computer based information systems and data. These can be found at <http://www.canterbury.ac.uk/support/student-support-services/students/disciplinary.doc>
- 3.6 All users who access any system or network beyond the University are automatically bound by the JANET Acceptable Use Policy. This is available from <http://www.ja.net/company/policies/janet-aup.html>
- 3.7 Users of any IT facilities provided jointly with another University or organisation are bound by both the specific regulation for that facility and these regulations.

4 User Management and Registration

- 4.1 No person shall use any University IT facility unless they have been appropriately and individually authorised.
- 4.2 User Management is based on data held within three Corporate Information Systems' (CIS) databases; Student records, Human Resources and Associates databases. All user accounts and permissions will be predicated on information held within these three central databases.

The process of account management will ensure that only authorised staff, students and associates have accounts. The process will clearly allocate and remove privileges in a consistent and accountable manner.

- 4.3 All accounts will have a defined lifetime or be tied to the continued existence of a live record in one of the three CIS databases listed above; extension will be only permitted by appropriately authorised and accountable staff. All accounts once expired will be formally removed from the systems by an automated process.
- 4.4 Student accounts will be created solely on the basis of information held in the student record system. Permissions will be dependant on the programmes / modules on which a student is enrolled and have a defined life related to the programme or module end date. When a student leaves the University their account will be disabled for a defined period after which it will be deleted.
- 4.5 Staff accounts will be based on the information held in the Human Resources record system. Permissions will be dependant on the position a staff member has and have a finite life which will be related to position end date or end of employment. When a member of staff leaves the employ of the University their account will be disabled for a defined period after which it will be deleted. Additional permissions may be added by an authorised person in respect of specific roles and responsibilities not related to the post.
- 4.6 Associates use of computer based services is dependant on the type of relationship with the University and have a defined life related to the activity.
- 4.7 Staff and students will have an account created automatically, based on the data held. The details of this will be given to the user during their induction process.
- 4.8 Requests for registration by an associate shall be in the appropriate form and shall include details of the requester, the IT facilities required including any necessary details of type or scope of access, and the period for which access is requested.
- 4.9 Registration to use IT facilities or the use of IT facilities constitutes acceptance of these regulations.
- 4.10 All authorised users shall be allocated a user account, which, together with any facilities authorised, may only be used for the purposes for which they have been allocated. This account will normally consist of a username, password and email address.
- 4.11 All individually allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they are allocated, as are any individually allocated certificates. The user is personally responsible and accountable for all activities carried out under their username.
- 4.12 Users must not use another user's account or password, nor allow any password issued to them to become known to any other person, nor, having logged in, leave IT facilities unattended and potentially usable by some other person.
- 4.13 Users must notify the University of any change in their status which may affect their right to use IT facilities, except students completing their registration.

5 Purpose of Use

- 5.1 University IT facilities are provided to enable a person to undertake work as an employee, studies as a student, or other associated role.

- 5.2 Use for other purposes, such as personal electronic mail or recreational use of the World Wide Web, is a privilege, which can be withdrawn. Any such use must be in keeping with these regulations and must not interfere with the user's duties or studies or any other person's use of IT facilities and must not, in any way, bring the University into disrepute. Priority must always be granted to those needing facilities for the work of the University.
- 5.3 University e-mail addresses and associated University e-mail systems must be used for all official University business transacted via e-mail, in order to facilitate audit and University record keeping. All staff and students of the University must regularly read their University e-mail.
- 5.4 Commercial or consultancy work for outside bodies, using University IT facilities, requires explicit permission from the designated authority. Such use may be liable to charge. It must be noted that the terms of University software licences (including Microsoft Windows and Office) are for educational use only, and so commercial use may be impossible without significant additional cost.
- 5.5 The use of IT facilities to the substantial advantage of other bodies such as employers of placement students must have the explicit prior permission of the designated authority and may be subject to charge.
- 5.6 The use of IT facilities by persons other than registered users must have the explicit prior permission of the designated authority and may be subject to charge. A process exists to register short term accounts for conferences and other legitimate activity.

6 Acceptable Use

The following lists are not exhaustive but give examples of activities which would normally be considered breach of these regulations.

Users must not:-

- 6.1 in any way cause any form of damage to the University's IT facilities, to any of the areas which accommodate those facilities, nor to any services associated with them.
- 6.2 modify any software nor incorporate any part of the provided software into their own work without permission from the designated authority.
- 6.3 load onto the IT facilities any software without permission from the designated authority.
- 6.4 deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the University to prevent this.
- 6.5 delete or amend the data or data structures of other users without their permission.
- 6.6 exceed the terms of their registration in their use of IT facilities
- 6.7 move any equipment or other IT facility without the prior agreement of the designated authority.
- 6.8 attempt to gain access to, copy, or otherwise make use of any other user's program or data. This includes acquiring knowledge of any other user's password.
- 6.9 disclose their usernames or passwords to any other person, nor shall they use or attempt to use any system which they have not been authorised to access.
- 6.10 attempt to gain access to systems management facilities or other facilities not available for general use.
- 6.11 use IT facilities to display, print, transmit or store text or images or other data which could be considered offensive such as pornographic, racially abusive or libellous material.
- 6.12 make use of the University's IT facilities to harass any person or group of persons.
- 6.13 produce, use or promulgate material via the University's IT facilities which could bring the University, or any part of the University, into disrepute. Where such a question might arise prior permission should be sought in writing from the appropriate SMT member
- 6.14 make any use of the University's IT facilities to undertake or assist in a criminal act.

- 6.15 send unsolicited bulk email; this includes but is not limited to advertisements and political and religious materials.
- 6.16 download, distribute, or store music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- 6.17 distribute or store by any means any pirated software;
- 6.18 monitor or intercept network traffic, without explicit permission
- 6.19 probe for security weaknesses of systems by any method (e.g. port-scanning) without explicit permission;
- 6.20 download, adapt, create or supply any software or system that could be used to obtain unauthorised access or prevent access to any computer system, unless with explicit permission as part of academic study,
- 6.21 undertake any activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs;
- 6.22 make excessive use of resources such as filestore, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- 6.23 pass on electronic chain mail;
- 6.24 make use of the University's IT facilities to post defamatory comments about staff or fellow students on virtual learning environment or social networking sites;
- 6.25 use University business mailing lists for non-academic purposes;
- 6.26 use CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.;
- 6.27 copy other people's web site material without the express permission of the copyright holder;
- 6.28 intentionally use other people's material without attribution (see the University plagiarism policy)
- 6.29 use peer-to-peer and related applications within the University. (These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA)
- 6.30 connect an unauthorised device to the University network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, IT purchasing policy, and acceptable use.

Users must

- 6.31 adhere to the terms and conditions of all licence agreements relating to IT facilities which they use including software, equipment, services documentation and other goods.
- 6.32 obey any published rules and policies for the use of networks and remote IT facilities
- 6.33 ensure that they start and terminate each session of use of IT facilities in accordance with published instructions.
- 6.34 only inspect and view Corporate or confidential information when doing so is necessary to perform their duties and there is a clear business requirement to do so.
- 6.35 never disclose or discuss data held in any Corporate system with colleagues, or external bodies unless doing so is directly related to their duties and does not break the Data Protection Act.

7 Student Open Computing Areas

7.1 Users must not:

- 7.1.1 interfere with the use by others of the IT facilities;
- 7.1.2 remove or interfere with output belonging to another user.
- 7.1.3 make frivolous use of University owned Computing areas, especially where such activities interfere with others' legitimate use of IT services;

7.2 Users must

- 7.2.1 take every precaution to avoid damage to equipment caused by smoking, eating or drinking in its vicinity.

- 7.2.2 respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT facilities.
- 7.2.3 respect published times for access to IT facilities.
- 7.2.4 minimise the use of consumables such as paper, and dispose of scrap paper tidily and to reduce any possible fire risk.

8 *Disciplinary Action*

- 8.1 The University reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and / or other contraventions of this policy.
- 8.2 Any attempt or actual breach of security or discipline may lead to the suspension or withdrawal of a user's authorisation and shall constitute an offence under the University's disciplinary regulations. Staff or students who break the Acceptable Use Regulations will be subject to the University's disciplinary procedures.
- 8.3 These regulations form part of the terms and conditions of appointment of members of staff and breaches of the regulations may be dealt with under the disciplinary procedures contained in those terms and conditions.

9 *Privacy and Monitoring*

- 9.1 The University fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit, in line with its rights under relevant legislation.
- 9.2 Systems staff who have appropriate privileges have the ability, which is occasionally required, to access all files, access logs and electronic mail files stored on IT facilities. It is also occasionally necessary to intercept network traffic.
- 9.3 Reasons for such monitoring may include:
 - The need to ensure operational effectiveness of services,
 - To prevent or investigate a breach of the law, this policy, or other University policy,
 - the investigation of an incident e.g. alleged contravention of University rules, regulations, contracts, codes etc or alleged criminal activity
 - the investigation of abnormal systems behaviour in an operational context e.g. abnormally high network traffic from a particular device, degradation of systems for other users resulting from the activity on a specific device etc
 - problem-solving e.g. ensuring a file transfer takes place; the user would normally instigate this but, on occasions, the intended recipient raises the query and the sender is unavailable
- 9.4 In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of service users. This policy on the privacy and the interception of electronic communications is intended to achieve a balance between the rights of individuals and the need to protect users and the University from the consequences of misuse or illegal activity.

10 *Chargeable Services*

- 10.1 Charges may be made for registration and/or for some or all use of IT facilities. All such charges will be listed on the Computing Services web site, and approved by the Information Systems Committee.

- 10.2 All usage for private purposes and all usage in connection with consultancy or research projects for which outside funds for computing costs are available, shall be declared as such; a charge may be levied for such usage.
- 10.3 Any financial or commercial advantage arising out of the use of computing resources shall be reported immediately, irrespective of when this advantage would arise and of who should benefit
- 10.4 Users will be charged for the full cost, as determined by the designated authority, of remedying any damage they cause.

Appendix A

The following message will appear on all University personal computers at startup and all users will have to confirm acceptance before being able to log in:

Canterbury Christ Church University Legal Notice

IT facilities are provided for University purposes and for use by employees in accordance with their normal duties of employment and by students in connection with their University education. Such use is governed by English law and subject to the Regulations for the Acceptable Use of University Information Technology and the University Policy on Access to the Internet, which may be amended from time to time ; please see the web page <http://www.canterbury.ac.uk/legal>

The University may monitor your use of this system in accordance with relevant legislation. The University may take action in the case of misuse, any monitoring will be proportionate, necessary and in accordance with University Policy and Procedures.

In particular, the deliberate access to and retention or distribution of material that is unlawful; obscene or deliberately offensive in nature; discriminatory on grounds of age, disability, faith or belief, gender, race or sexual orientation; or likely to result in harassment or bullying of others will be treated as a contravention of University Policy.

Unauthorised access to any University IT facilities is forbidden, and will be deemed to be a breach of the Computer Misuse Act 1990.

Document control/change history				
Version	Author(s)	Date	Circulation	Comments
1	IE		ISC policy subgroup	First draft based on old doc
2	IE	1/5/08		major re-write to reflect current needs
3	IE	Aug/08	Policy sub-group	Further major re-write
4	IE/RM	Sept 08		Tidy up and edit
5	IE/RM	October 2008	ISC	final
5.1	IE/RM	October 2008	Academic Board	Minor change by ISC
5.2	IE/RM	December 2008	University	Minor change by Academic Board

Document ratification and history	
Approved by:	Information Systems Committee
Date approved:	29 October 2008
Review date:	1 October 2009
Author(s):	Ian Ellery
Owning Department:	Computing Services