ICTC Regulations 1 of 2002

Made by the ICTC on 6 June 2002

Approved by Council on 24 July 2002
Amended on 2 October 2003, 23 October 2003, 16 February 2006, 1 June 2006, 3 June 2010 and 19 July 2012

1. In these regulations, unless the context requires otherwise, 'college' means any college, society, or Permanent Private Hall or any other institution designated by Council by regulation as being permitted to present candidates for matriculation.

2. University IT and network facilities are provided for use in accordance with the following policy set by Council:

(1) The University provides computer facilities and access to its computer networks only for purposes directly connected with the work of the University and the colleges and with the normal academic activities of their members.

(2) Individuals have no right to use university facilities for any other purpose.

(3) The University reserves the right to exercise control over all activities employing its computer facilities, including examining the content of users' data, such as e-mail, where that is necessary:

(*a*) for the proper regulation of the University's facilities;

(*b*) in connection with properly authorised investigations in relation to breaches or alleged breaches of provisions in the University's statutes and regulations, including these regulations; or

(*c*) to meet legal requirements.

(4) Such action will be undertaken only in accordance with these regulations.

3. These regulations govern all use of university IT and network facilities, whether accessed by university property or otherwise.

4. Use is subject at all times to such monitoring as may be necessary for the proper management of the network, or as may be specifically authorised in accordance with these regulations.

5. (1) Persons may make use of university facilities only with proper authorisation.

(2) 'Proper authorisation' in this context means prior authorisation by the appropriate officer, who shall be the Chief Information Officer or his or her nominated deputy in the case of services under the supervision of IT Services, or the nominated college or departmental officer in the case of services provided by a college or department.

(3) Any authorisation is subject to compliance with the University's statutes and regulations, including these regulations, and will be considered to be terminated by any breach or attempted breach of these regulations.

6. (1) Authorisation will be specific to an individual.

(2) Any password, authorisation code, etc. given to a user will be for his or her use only, and must be kept secure and not disclosed to or used by any other person. Exceptions may be made for accounts set up specifically to carry out business functions of the University or a unit within it, but authorisation must be given by the head of the unit.

7. Users are not permitted to use university IT or network facilities for any of the following:

(1) any unlawful activity;

(2) the creation, transmission, storage, downloading, or display of any offensive, obscene, indecent, or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the use of the facilities for properly supervised research purposes when that use is lawful and when the user has obtained prior written authority for the particular activity from the head of his or her department or the chairman of his or her faculty board (or, if the user is the head of a department or the chairman of a faculty board, from the head of his or her division);

(3) the creation, transmission, or display of material which is designed or likely to harass another person in breach of the University's Code of Practice on Harassment;

(4) the creation or transmission of defamatory material about any individual or organisation;

(5) the sending of any e-mail that does not correctly identify the sender of that e-mail or attempts to disguise the identity of the computer from which it was sent;

(6) the sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person;

(7) the transmission, without proper authorisation, of e-mail to a large number of recipients, unless those recipients have indicated an interest in receiving such e-mail, or the sending or forwarding of e-mail which is intended to encourage the propagation of copies of itself;

(8) the creation or transmission of or access to material in such a way as to infringe a copyright, moral right, trade mark, or other intellectual property right;

(9) private profit, except to the extent authorised under the user's conditions of employment or other agreement with the University or a college; or commercial purposes (including advertising commercial services) without specific authorisation;

(10) gaining or attempting to gain unauthorised access to any facility or service within or outside the University, or making any attempt to disrupt or impair such a service;

(11) the deliberate or reckless undertaking of activities such as may result in any of the following:

(*a*) the waste of staff effort or network resources, including time on any system accessible via the university network;

(*b*) the corruption or disruption of other users' data;

(*c*) the unauthorised access, transmission or negligent loss of data;

(*d*) the violation of the privacy of other users;

(*e*) the disruption of the work of other users;

(*f*) the introduction or transmission of a virus or other malicious software into the network;

(12) activities not directly connected with employment, study, or research in the University or the colleges (excluding reasonable and limited use for social and recreational purposes where not in breach of these regulations or otherwise forbidden) without proper authorisation.

8. Software and computer-readable datasets made available on the university network may be used only subject to the relevant licensing conditions, and, where applicable, to the Code of Conduct published by the Combined Higher Education Software Team ('CHEST').

9. Users shall treat as confidential any information which may become available to them through the use of such facilities and which is not clearly intended for unrestricted dissemination; such information shall not be copied, modified, disseminated, or used either in whole or in part without the permission of the person or body entitled to give it.

10. (1) No user may use IT facilities to hold or process data relating to a living individual save in accordance with the provisions of current data protection legislation (which in most cases will require the prior consent of the individual or individuals whose data are to be processed).

(2) Any person wishing to use IT facilities for such processing is required to inform the University Data Protection Officer in advance and to comply with any guidance given concerning the manner in which the processing may be carried out.

11. Any person responsible for the administration of any university or college computer or network system, or otherwise having access to data on such a system, shall comply with the provisions of the 'Statement of IT Security and Privacy Policy'.

12. Users shall at all times endeavour to comply with policies and guidance issued from time to time by IT Services to assist with the management and efficient use of the University's ICT facilities.

13. Connection of any computer, whether college, departmental, or privately owned, to the university network is subject to the following additional conditions:

(1) (*a*) Computers connected to the university network may use only network identifiers which follow the University's naming convention, and are registered with IT Services.

(*b*) The University's Trade Mark and Domain Name Policy specifies, *inter alia*, that all university activities (other than those within OUP's remit) should be presented within the ox.ac.uk domain. Any exception to this requires authorisation as defined in that Policy.

(2) (*a*) Owners and administrators of computers connected to the university network are responsible for ensuring their security against unauthorised access, participation in 'denial of service' attacks, etc. In particular they are responsible for ensuring that anti-virus software is installed and regularly updated, and that rules and guidelines on security and anti-virus policy, as issued from time to time by IT Services, are followed.

(*b*) The University may temporarily bar access to any computer or sub-network that appears to pose a danger to the security or integrity of any system or network, either within or outside Oxford, or which, through a security breach, may bring disrepute to the University.

(3) (*a*) Providers of any service must take all reasonable steps to ensure that that service does not cause an excessive amount of traffic on the University's internal network or its external network links.

(*b*) The University may bar access at any time to computers which appear to cause unreasonable consumption of network resources.

(4) (*a*) Hosting Web pages on computers connected to the university network is permitted subject to the knowledge and consent of the department or college responsible for the local resources, but providers of any such Web pages must endeavour to comply with guidelines published by IT Services or other relevant authorities.

(*b*) It is not permitted to offer commercial services through Web pages supported through the university network, or to provide 'home-page' facilities for any commercial organisation, except with the permission of the Chief Information Officer (IT Services); this permission may require the payment of a licence fee.

(5) Use of file-sharing technology and participation in distributed file-sharing networks may be subject to additional regulation and restriction in order to prevent excessive use of university network resources, or the use of those resources for purposes unconnected with the University. If a user has any reason to suppose that an application employs peer-to-peer (p2p) or other file-sharing technology, they should seek the advice of the IT officer responsible for the college or departmental network on which they propose to use the software.

(6) (*a*) No computer connected to the university network may be used to give any person who is not a member or employee of the University or its colleges access to any network services outside the department or college where that computer is situated.

(*b*) Certain exceptions may be made, for example, for members of other UK universities, official visitors to a department or college, or those paying a licence fee.

(*c*) Areas of doubt should be discussed with the Head of IT Services.

(7) Providing external access to University network resources for use as part of any shared activity or project is permitted only if authorised by the IT Committee (ITC), and will be subject to any conditions that it may specify.

(8) If any computer connected to the network or a sub-network does not comply with the requirements of this section, it may be disconnected immediately by the Network Administrator or any other member of staff duly authorised by the head of the college, section or department concerned.

14. (1) If a user is thought to be in breach of any of the University's statutes or regulations, including these regulations, he or she shall be reported to the appropriate officer who may recommend to the appropriate university or college authority that proceedings be instituted under either or both of university and college disciplinary procedures.

(2) Access to facilities may be withdrawn under section 42 of Statute XI pending a determination, or may be made subject to such conditions as the Proctors or the Registrar (as the case may be) shall think proper in the circumstances.

Examining Users' Data

15. All staff of an IT facility who are given privileged access to information available through that facility must respect the privacy and security of any information, not clearly intended for unrestricted dissemination, that becomes known to them by any means, deliberate or accidental.

16. (1) System Administrators (i.e. those responsible for the management, operation, or maintenance of computer systems) have the right to access users' files and examine network traffic, but only if necessary in pursuit of their role as System Administrators.

(2) They must endeavour to avoid specifically examining the contents of users' files without proper authorisation.

17. (1) If it is necessary for a System Administrator to inspect the contents of a user's files, the procedure set out in paragraphs (2)-(5) below must be followed.

(2) Normally, the user's permission should be sought.

(3) Should such access be necessary without seeking the user's permission, it should, wherever possible, be approved by an appropriate authority prior to inspection.

(4) If it has not been possible to obtain prior permission, any access should be reported to the user or to an appropriate authority as soon as possible.

(5) For the purposes of these regulations 'appropriate authority' is defined as follows:

(*a*) in the case of any university-owned system, whether central or departmental: if the files belong to a student member, the Proctors; if the files belong to any member of the University other than a student member, the Registrar or his or her nominee; or, if the files belong to an employee who is not a member of the University, or to a visitor to the University, the head of the department, college, or other unit to which the employee or visitor is responsible, or the head's delegated representative;

(*b*) in the case of a departmental system, either those named in (*a*) above, or, in all circumstances, the head of department or his or her delegated representative;

(*c*) in the case of a college system, the head of the college or his or her delegated representative.