University Policies in Data Protection

DATA PROTECTION POLICY

The primary purpose of current data protection legislation is to protect individuals against possible misuse of information about them held by others. Under the provisions of the Data Protection Act 1984, specific legislation was introduced in relation to automated data. The impact of the legislation was considerably widened under the terms of the Data Protection Act 1998 which came into force on the 1 March 2000. It is the policy of the University to ensure that all members of the University and its staff are aware of the requirements of data protection legislation under their individual responsibilities in this connection.

The new Act covers personal data, whether held on computer or in a "relevant filing system". The University is obliged to abide by the data protection principles embodied in the Act. These principles require that personal data shall:

- Be processed fairly and lawfully
- Be held only for specified purposes and not used or disclosed in any way incompatible with those purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up-to-date
- Not be kept for longer than necessary for the particular purpose
- Be processed in accordance with data subject's rights
- Be kept secure
- Not be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection

Guidance on what constitutes fair and lawful processing (principle 1) can be found at: http://www.admin.ox.ac.uk/councilsec/oxonly/dp/defs.shtml

The Act provides individuals with rights in connection with personal data held about them. It provides individuals with the right to access data concerning themselves (subject to relevant *transitional relief* and the rights of third parties). It also includes the right to seek compensation through the courts for damages and distress suffered by reason of inaccuracy or the unauthorised destruction or wrongful disclosure of data. Access requests should be addressed to the University's Data Protection Officer (Jennifer Noon, University Offices).

Under the terms of the new Act, processing of data includes any activity to do with the data involved. All staff or other individuals who have access to, or who use, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised person. Examples of data include address lists and contact details as well as individual files. Any processing of such information must be done in accordance with the principles outlined above. In order to comply with the first principle (fair and lawful processing), at least one of the following conditions must be met:

- The individual has given his or her consent to the processing
- The processing is necessary for the performance of a contract with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the controller or third parties (unless it could prejudice the interests of the individual)

In the case of *sensitive personal data*, which includes information about racial or ethnic origins; political beliefs; religious or other beliefs; trade union membership; health; sex life; criminal allegations, proceedings or convictions, there are additional restrictions and explicit consent will normally be required.

In relation to security (Principle 7), the Data Controller (the University) must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data and sets out specific considerations for ensuring security. Staff and other individuals should be aware that guidelines and regulations relating to the security of manual filing systems and the preservation of secure passwords for access to relevant data held on computer should be strictly observed.

Staff should also note that personal data should not normally be provided to parties external to the University. Special arrangements apply to the exchange of data between the University and the colleges. For further guidance on this, please contact: data.protection@admin.ox.ac.uk

Under principle 8, which restricts the transfer of material outside the European Area, personal data about an individual placed on the world wide web is likely to breach the provisions of the Act unless the individual whose data is used has given his or her express consent. It is important that all those preparing web pages, address lists and the like, are aware of these provisions, and seek advice from the Data Protection Officer if in doubt.

The Act specifies arrangements for the notification of processing undertaken by the Institution. The University has a wide ranging notification under the 1998 Act, which can be accessed online via: http://www.dpr.gov.uk/search.html. Any members of staff or individuals who are uncertain as to whether their activities or proposed activities are included in the University's notification should contact the Data Protection Officer in the first instance.

A failure to comply with the provisions of the Act may render the University, or in certain circumstances the individuals involved, liable to prosecution as well as giving rise to civil liabilities. Individuals are encouraged to familiarise themselves with the general aspects of Data Protection contained in the University's guidelines to the Act, referred to above and with any specific measurements recommended by the University or their Department relevant to the particular nature of their work. Further information and advice may be obtained from Departmental Data Protection Representatives or from the University's Data Protection Officer – please send enquiries to: data.protection@admin.ox.ac.uk.

UNIVERSITY RULES FOR COMPUTER USE

Policy Statement on Computer Use, Monitoring, and Surveillance

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

‘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. Individuals have no right to use University facilities for any other purpose.

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 authorized investigations in relation to breaches or alleged breaches of provisions in the University’s statutes, decrees and regulations, and the rules on computers use published by the Information and Communications Technology (ICT) Committee from time to time; or

(c) to meet legal requirements.

Such action will only be undertaken in accordance with guidelines laid down and published from time to time by the ICT Committee.’

Rules Governing IT Use

The following rules govern all use of University IT and network facilities, whether accessed by University property or otherwise.

(1) 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 authorized in accordance with rules laid down from time to time by the ICT Committee for the purpose of investigation of allegations of activity in breach of the law, or of the University’s statutes, decrees and regulations.

(2) Persons may only make use of University facilities with proper authorization. *Proper authorization* in this context means prior authorization by the appropriate officer, who shall be the Director of OUCS or his or her nominated deputy, in this case of services under the supervision of OUCS, or the nominated college or departmental officer in the case of services provided by a college or department. Any authorization is subject to compliance with these rules, and with the University’s statutes, decrees and regulations, and will be considered to be terminated by any breach or attempted breach of these rules.

(3) Authorisation will be specific to an individual, 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.

(4) Users are permitted to use University IT or network facilities for any of the following:

(a) any unlawful activity;

(b) 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;

(c) the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety, or to harass another person;

(d) he creation or transmission of defamatory material about any individual or organisation;

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

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

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

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

(i) 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 without specific authorisation;

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

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

I the waste of staff effort or network resources, including time on any system accessible via the University’s network;

II the corruption or disruption of other users’ data:

III the violation of the privacy of other users;

IV the disruption of the work of other users;

V the introduction or transmission of a virus into the network

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

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

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

(7) 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 is to be processed). 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.

(8) Any person responsible for the administration of any University or college computer or network system, otherwise having access to data on such a system, shall comply with the provisions of the 'Statement of IT Security and Privacy Policy' as published by the ICT Committee from time to time.

(9) Users shall at all times endeavour to comply with guidance issued from time to time by OUCS to assist with the management and efficient use of the network.

(10) Connection of computers, whether college, departmental or privately owned, to the University network is subject to the following additional regulations:

(a) Computers connected to the University network may only use network identifiers which follow the University's naming convention, and registered with OUCS. In particular all such names must be within the domain .ox.ac.uk. Any exception to this must be authorized by the Director of OUCS, and may be subject to payment of a license fee.

(b) The administrators of computers connected to the University network are responsible for ensuring their security against unauthorized access,

participation in ‘denial of service’ attacks, etc. 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.

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

(d) 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 these web pages must endeavour to comply with guidelines published by OUCS or other relevant authorities. It is not permitted to offer commercial services through the web pages supported through the University network, or to provide “home-page” facilities for any commercial organization, except with the permission of the Director of OUCS. This permission may require the payment of a licence fee.

(e) Participation in distributed file-sharing networks in circumstances where there is no clear academic purpose is not permitted.

(f) 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 college’s access to any network services outside the department or college where that computer is situated. Certain exceptions may be made, for example members of other UK Universities, official visitors to a department or college, or for those paying a licence fee. Areas of doubt should be discussed with the Registration Manager at OUCS.

(11) In the event that a user is thought to be in breach of one or more of these rules or of University statutes, decrees, or 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 University or College disciplinary procedures. Access to facilities may be withdrawn pending a determination, or may be made subject to such conditions as the appropriate officer shall think proper in the circumstances.

[1] This rule is not intended to prevent the use of the facilities for properly supervised research purposes, provided that the use is lawful and that the user has obtained prior authority for the particular activity in the manner set out from time to time by the ICT Committee.

Guidelines for Examining Users' Data

(1) 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 intended for public dissemination, that becomes known to them by any means, deliberate or accidental.

(2) 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 Administrator. They must endeavour to avoid explicitly examining the content of users' files without proper authorisation.

(3) If it is necessary for a System Administrator to inspect the contents of users' files, the following procedure must be followed. Normally, the users' permission should be sought. Should such access be necessary without seeking the users' permission, it should, wherever possible, be approved by an appropriate authority prior to inspection. 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.

(4) For the purposes of these guidelines *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, the proctors; if the files belong to a Senior Member, the Registrar or his or her nominee; or, if the files belong to an employee who is not a Senior Member, the Head of the Department, House or other unit to which the employee is responsible, or his or her delegated representative;

(a) In the case of a departmental system, either those named in *(a)*, or, in all circumstances, the Head of Department or his or her delegated representative;

(b) In the case of a college system, the Head of House or his or her delegated representative.

Note: the above rules incorporate amendments made by council on 18 June 2001. Further changes may be made at any time. An up to date copy of these rules may be found at http:/www.ox.ac.uk/it/rules.html