

**UNIVERSITY OF
BIRMINGHAM**

IT Services

**General Conditions of Use
of
Computing and Network Facilities**

GENERAL CONDITIONS OF USE OF COMPUTING AND NETWORK FACILITIES

Contents

- 1. Introduction and Scope**
- 2. Data Protection Act 1998**
- 3. Licence Registration and Prevention of Piracy**
- 4. Commercial Exploitation of Inventions/Intellectual Property**
- 5. Security of Computer Information**
- 6. Use of Email and Electronic Means of Publication**
- 7. General Conditions Relating to Use of Specific Systems**
- 8. Consent to Intercept and Disclose Data**
- 9. Disciplinary Offences**
 - 9.1 General
 - 9.2 Hacking and Viruses
 - 9.3 Infringement of Software Licences and Copyright
 - 9.4 Offensive, Indecent and Defamatory Material and Messages
 - 9.5 Network Management and Network Security
 - 9.6 Wilful Damage
 - 9.7 Unsolicited Bulk Email
 - 9.8 Harassment
 - 9.9 Access to Data
 - 9.10 Impersonation
 - 9.11 Disciplinary Offences Committed External to the University
 - 9.12 Further Action
- 10. Other Matters**
 - 10.1 University Liability
 - 10.2 Additional Information
- 11. Centrally Provided Computing Facilities**
 - 11.1 Introduction and Scope
 - 11.2 Registration and Use
 - 11.3 Equipment
 - 11.4 Further Conditions

General Conditions of Use of Computing and Network Facilities

1. Introduction and Scope

The General Conditions of Use of Computing and Network Facilities form part of the conditions of employment which all staff are required to observe. This includes observance of the University's Information Security Policy and associated Codes of Practice.

For the purposes of Ordinances on Student Discipline, these Conditions of Use have the status of a Code of Practice approved by Council (Ordinance 5.5.2 (i) and 5.6.3 (a) (i)).

The General Conditions of Use apply to all computer users and to all computer equipment within or operated by the University. This includes all staff, students and any third parties who have been granted access to University computing facilities or data.

In these General Conditions of Use, 'computer', 'computer system' and 'computer network' mean those which are in one or more of the following categories:

- i. the property of the University or leased/rented to it
- ii. on loan to the University from third parties
- iii. the property of parties to University contracts located in the University, or attached to University computers, computer systems or computer networks
- iv. used on the University network, irrespective of ownership
- v. used to gain access to University computing and network facilities or systems, irrespective of ownership, and 'computing and/or network resources' means any such property

The University Network includes all communication equipment which transmits information electronically.

Section 11 defines Conditions of Use particularly relevant to centrally provided computing facilities.

2. Data Protection Act 1998

Every person shall comply with the requirements of the Data Protection Act 1998 ("the Act") concerning personal data. The Act enunciates eight principles relating to the collection, keeping and disclosure of personal data:

- i. data shall be obtained and processed fairly and lawfully
- ii. data shall only be held for specified and lawful purposes
- iii. data shall not be used or disclosed except in accordance with the Act
- iv. data shall be adequate, relevant and not excessive for those purposes
- v. data shall be accurate and up-to-date
- vi. data shall not be kept any longer than necessary
- vii. an individual has the right, at reasonable intervals and without undue delay or expense, to know what personal data may be held about him/her, to access those data, and (where appropriate) to have those data corrected or erased
- viii. security measures shall be taken to prevent unauthorised access to data and to prevent accidental loss or damage.

It is a criminal offence to disclose another individual's personal data, unless the disclosure is with consent or in one of the specified limited circumstances in the Act.

Every person contemplating the collection, storage or use of personal data must consult the University Data Protection Officer before such collection, storage or use, and must follow the registration procedure adopted by the University. This applies irrespective of the ownership of the computer on which it is intended to store the data. All members of the University must also comply with the University's Data Protection Policy available at: http://www.legalservices.bham.ac.uk/data_protection_policy/

3. Licence Registration and Prevention of Piracy

All licences concerning hardware and software must be registered and where appropriate signed by an authorised signatory within the College, School or Budget Centre.

Where software has been electronically downloaded from IT Services computer systems requiring user authentication by means of a username and password, the user must read and comply with the licensing conditions for that software, and the act of downloading indicates acceptance of the licensing conditions pertinent to that software.

Similarly where software has been electronically downloaded from sites elsewhere on the Internet, the act of downloading indicates acceptance of the licensing conditions pertinent to that software. Before downloading the software ensure that the licensing conditions have been read and do not conflict with University policy or interests.

Where the software is required by University staff, any legal queries should be referred to Legal Services prior to downloading.

Registration and signature will occur at Budget Centre or University level depending on the nature of the licence.

All persons who are licensed to use software or who control access to any computing and/or network resources are obliged to take all reasonable care to prevent the illicit copying and use of software and documentation.

No one shall introduce onto computer systems any software or other material requiring a licence for which a valid licence is not in place.

The University reserves the right for access to be granted to computer audit staff without notice to enable them to check against an inventory of licensed software and hardware. Any unlicensed software or hardware or illicit copies of documentation will be removed by such audit staff and reported to the Director of IT Services, who may initiate disciplinary proceedings.

4. Commercial Exploitation of Inventions/Intellectual Property

The commercial exploitation of software or hardware developed using University computing and/or network resources must be referred to the University's Licensing Manager (c/o Birmingham Research and Development Limited) for the proper construction of a Licence, in accordance with the Employees Terms and Conditions of Employment or for students in accordance with Regulation 5.3 or such other regulation as may be in force from time to time.

As specified in Regulation 5.3 copyright in software produced or developed by students will be assigned to the University. Students will in consideration of such assignments be afforded the same rights as members of staff as laid down in the University Regulation 'Patents and the Exploitation of Inventions'.

5. Security of Computer Information

All persons responsible for computer equipment of any type must take adequate precautions to ensure that the physical environment is secure in order to prevent illegal access to equipment and/or theft. The level of physical security should be appropriate to the type and location of the equipment.

In all instances where sensitive data of any kind are held, irrespective of whether or not Data Protection legislation applies, every effort must be taken to ensure that the data are secure. In this context data include passwords and other levels of access security, and the threat to secure data includes the possible introduction of viruses.

All important data must be appropriately backed up to guard against media or mechanical failure. A suitable backup strategy and implementation must be adopted appropriate to the type and location of the equipment.

All computer procedures and data are subject to review by the University's Internal and/or External Auditors without notice, and in particular the Internal Auditor is responsible for periodically reviewing adherence to computer security policy and assessing the appropriateness of security measures at a local level.

Further guidance on security of computer information and what constitutes reasonable measures appropriate to various types of computer equipment can be found in the University's Information Security Policy and associated Codes of Practice.

6. Use of Email and Electronic Means of Publication

All members of the University shall comply with the Code of Practice relating to the monitoring of emails.

Unless specifically stated, all views and opinions expressed by members of the University within email messages and other means of electronic publication (such as personal web pages) are the individual's own, and do not reflect any official position of the University of Birmingham.

Deliberate use of obscene, pornographic, offensive or defamatory language or imagery is a disciplinary offence and may result in the withdrawal of computing facilities in addition to disciplinary proceedings.

Use of copyrighted material, trade marks, or other intellectual property without consent of the owner is also a disciplinary offence and may result in the withdrawal of computing facilities in addition to disciplinary proceedings.

7. General Conditions Relating to Use of Specific Systems

Every person who connects to and uses computing and/or network resources owned or controlled by the University shall abide by the General Conditions of Use, the Information Security Policy and associated Codes of Practice, as well as satisfying the registration conditions currently in force in respect of the Budget Centre(s) controlling the use of the equipment or associated facilities. The provisions in any local Conditions of Use which may be drawn up shall not override the provision in these General Conditions of Use.

University computing and/or network resources are provided for University purposes which means those purposes concerned with undergraduate, postgraduate or other courses, research, personal education, development, administration, or other work authorised by the appropriate Head of Budget Centre.

Persons connecting to and using computing and/or network resources external to the University must abide by any conditions of use and satisfy any registration conditions imposed by the external agency such as the JANET UK Acceptable Use Policy.

All users must act so as to cause as little inconvenience or nuisance to other users as possible. All users must co-operate with other users and ensure equitable use of shared resources.

8. Consent to Intercept and Disclose Data

Use of University computer and computer network facilities is subject to the condition that users give express consent to the examination of any data stored in computers or computer systems and to the examining, monitoring and interception of data, communications or contents of computers by the University for lawful purposes whenever it is deemed necessary, together with the authority to pass such data legally to third parties either as required by law or to fulfil the University's contractual obligations relating to the Network. This work is normally carried out by IT Services on behalf of the University in order to meet operational and security needs of the University and related investigatory activities.

9. Disciplinary Offences

9.1 General

Breach of the Conditions of Use is a disciplinary offence which may result in the suspension of access to the Network and University Computing facilities and further disciplinary proceedings. The following are also disciplinary offences:

- i. Incitement to conduct leading to a breach of any provision of these General Conditions of Use shall itself constitute a disciplinary offence
- ii. Failure to comply with relevant English and European law while using or accessing the University computing or networking facilities constitutes a disciplinary offence
- iii. Failure to comply with the conditions of Section 11 (Centrally Provided Computing Facilities) is also a disciplinary offence.

9.2 Hacking and Viruses

Any person who wilfully and knowingly gains unauthorised access to a computer system or attempts to disable a computer system commits a disciplinary offence.

Any person who wilfully, knowingly and without authorisation introduces or attempts to introduce a virus or other harmful or nuisance program or file, or to modify or destroy data, programs or supporting documentation residing on, or existing internal or external to a computer, computer system or computer network commits a disciplinary offence.

Any person who wilfully, knowingly and without authorisation denies access or attempts to deny access or otherwise interferes with the legitimate operation of computers or computer systems, or uses any University computer, computer system or computer network to carry out such actions against an external computer system, commits a disciplinary offence.

9.3 Infringement of Software Licences and Copyright

Any person who wilfully, knowingly and without authorisation uses a computer, computer system or computer network to access, disclose, publish, take or copy programs data or supporting documentation or any other material or attempts to do so in infringement of intellectual property rights, licence conditions, contractual rights, copyright or confidentiality, wheresoever the act occurs, commits a disciplinary offence.

Where the University is rendered liable for any damages from such infringement, the University reserves the right to recover such damages from the person infringing the intellectual property rights, the licence conditions, the contractual rights copyright or confidentiality.

9.4 Offensive, Indecent and Defamatory Material and Messages

Disciplinary Offences

- (a) Any person who knowingly and without authorisation uses a computer, computer system or computer network to access or carry out any of the following activities commits a disciplinary offence, unless they are carried out under the provisions stated in paragraph (b) below:
- i. the creation, storage or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into offensive, obscene or indecent images or material
 - ii. the creation, storage or transmission of material which is designed to or is likely to cause annoyance, inconvenience or needless anxiety
 - iii. the creation, storage or transmission of defamatory material.

If staff or students create, store or transmit such material in the course of their research, permission must be sought in advance from the Director of IT Services prior to such action.

Exceptional Circumstances

- (b) Activities described in the preceding paragraph (a) may be allowed in the following circumstances:
- i. Staff specifically designated by the Director of IT Services to investigate security and other incidents, when their activities are in connection with those incidents
 - ii. Staff in the course of their recognised research, provided such research has been made known in advance to the Director of IT Services
 - iii. Students in the course of their supervised research, provided such research has been approved in advance by the Director of IT Services.

Social Networking Sites and Cyber Bullying

- (c) With reference to 9.4 (a), users are reminded that anyone who posts material attacking another member of the University on social networking sites in a way such as to bully or harass an individual, or bring the University into disrepute, may commit a disciplinary offence under the relevant University legislation.

9.5 Network Management and Network Security

Any unauthorised person who attempts to monitor traffic on the University Network or any person who attempts to connect an unauthorised device with the intention of monitoring traffic (ie eavesdropping) commits a disciplinary offence.

Any person who knowingly enters any restricted area without authorisation commits a disciplinary offence. For the purposes of this condition, restricted area includes all ducting and other containments or conduits carrying network equipment or cables.

9.6 Wilful Damage

Any person who negligently or by any wilful or deliberate act jeopardises the physical integrity of any computing and/or network resource, computer equipment, associated environmental conditioning equipment or physical network and power connections associated accommodation commits a disciplinary offence.

9.7 Unsolicited Bulk Email

Any person who sends unsolicited bulk email commits a disciplinary offence, unless it is for official University purposes, or being sent to a mailing list which has been set up with the consent of the list members and the email is consistent with the purpose of the mailing list. Care must be taken to ensure that bulk emailings comply with The Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Data Protection Act 1998 when applicable.

9.8 Harassment

Anyone who uses University computer and computer network facilities in order to carry out or facilitate racial, sexual or any other form of harassment commits a disciplinary offence.

9.9 Access to Data

Anyone who wilfully and knowingly acts to impede a security, disciplinary or operational investigation commits a disciplinary offence. This includes the removal or destruction of relevant data or hardware and the withholding of passwords and encryption keys.

9.10 Impersonation

Anyone who wilfully, knowingly and without authorisation makes use of a computer, computer system or computer network in order to impersonate another individual, company or administrative entity whether real or fictitious commits a disciplinary offence.

9.11 Disciplinary Offences Committed External to the University

Any person who wilfully, knowingly and without authorisation uses any computer, computer system or computer network originating in the University or connecting to any University computer, computer system or computer network to commit any of the actions listed above on a computer, computer system or computer network external to the University commits a disciplinary offence.

9.12 Further Action

In addition to any other disciplinary penalties applying to staff and those provided for under Regulations for student discipline, the University reserves the right to:

- i. deny all further access to relevant computer, computer systems and computer networks indefinitely or for a defined period of time
- ii. recover all reasonable costs howsoever incurred in investigating and subsequent restitution of computer, computer systems and computer networks resulting from any actions listed above
- iii. refer any possible criminal action to the police.

10. Other Matters

10.1 University Liability

The attention of users is drawn to the fact that the University will not accept liability for claims made by third parties arising out of the application and use of data, information or results obtained from University computing facilities.

The University accepts no responsibility for the loss of any data or software or the failure of any security or privacy mechanism.

Liability will only be accepted by the University for provision to third parties of computing and network resources where a contract to this effect has been negotiated and signed by the Registrar and Secretary.

10.2 Additional Information

The University Licensing Manager can be found in Birmingham Research and Development Limited.

The University Data Protection Officer can be found within Legal Services.

Copies of University Regulations are available on the University's web pages.

11. Centrally Provided Computing Facilities

11.1 Introduction and Scope

This Section applies to any 'computer', 'computer system' and 'computer network' under the central management or control of the University through IT Services. All users of such equipment are required to abide by the provisions of this Section, and all equipment covered by this Section is also covered by the terms of this document as a whole.

11.2 Registration and Use

11.2.1 All use of computing and/or network resources shall be made on the understanding that the use is for University purposes, and every registration of a user and subsequent allocation of computing and/or network resources shall be made on the understanding that use is for University purposes and solely for the registered user who is allocated the resource. Use shall not be made of resources allocated to another user unless such use is specifically authorised by the Director of IT Services. This Code of Practice prohibits a person from allowing a third party to make use of computing or network facilities in an unauthorised manner.

11.2.2 Where the University has specifically agreed that a contract or grant will involve the use of computing and/or network resources without payment, the level of resources to be provided must be agreed beforehand with the Director of IT Services. Where the University has specifically agreed that a contract or grant will involve payment for the use of computing and/or network resources, the rate of payment must be agreed beforehand with the Director of Finance; and the level of resources with the Director of IT Services.

- 11.2.3 Any other registered use may be the subject of a charge, to be agreed upon prior to registration, the user being personally liable to reimburse such charge. Failure to reimburse by the date specified will lead to the suspension of access for that use, until reimbursement is made.
- 11.2.4 Inappropriate use made by or authorised by staff or students of computing and/or network resources may constitute a disciplinary offence and may render the user or authoriser liable inter alia for reimbursement of charges incurred. This includes any activity which wastes significant University resources, including time of computer support staff.
- 11.2.5. Where registered users are allocated a computer identifier, they must use all reasonable endeavours to ensure that its integrity is maintained. Registered users must report any suspected breach of such security to the Director of IT Services immediately.

11.3 Equipment

- 11.3.1 No computer equipment or associated facilities may be removed from their location without authorisation. Authorisation must be obtained from the relevant Head of College, School or Budget Centre or their nominee. Users are responsible for and must take reasonable care of any facilities loaned to them and may be required to pay the value of any facility damaged or not returned.
- 11.3.2 Users must not interfere with the use by others of computing and/or network resources. In the event of suspected misuse of facilities by a user, the Director of IT Services may temporarily suspend use of or access to computing and/or network resources, pending further investigation.

11.4 Further Conditions

- 11.4.1 The above conditions may be supplemented from time to time by conditions relating to specific equipment made available on campus by special arrangements (eg Study Contracts with Computing Suppliers etc).

Mrs Gill Ball
Acting Registrar and Secretary
December 2007