

Conditions for Using Information Technology Facilities

Notes for Guidance

These notes provide guidance on the interpretation and application of the *Conditions for Using IT Facilities* [www.abdn.ac.uk/dit/policy.php] and are numbered according to the Conditions to which they refer. The Notes will be reviewed regularly and users will be notified of any significant changes.

Requests and queries relating to Directorate of Information Technology (DIT) administered services should normally be made through the DIT Service Desk (tel: x3636, e-mail: helpdesk@abdn.ac.uk).

1. & 1.1 University purposes

Application for special use or any concerns about the legitimacy of proposed use should be referred to the appropriate authority. Students should refer to their Supervisor or Class Tutor in the first instance. Charges, if any, will be set by the appropriate authority, subject to approval by the University Secretary.

1.2 Personal use

Guidelines for personal use of DIT-administered facilities are published at www.abdn.ac.uk/dit/policy.php. Publishing of personal WWW pages is permitted, subject to Condition #9. All personal use is prohibited at busy times in computer classrooms and clusters.

Any employee wishing to use IT facilities for personal purposes must ensure that permission has been obtained from his or her line manager.

2. Unacceptable use

Sending *spam* or chain e-mail will be regarded as harassment or offensive behaviour.

It is not the intention that these Conditions should be used to limit recognised academic freedom but that they should restrain unlawful, offensive or abusive use of University IT facilities. It is recognised that the ability to debate and examine contentious, uncomfortable or other difficult issues is an essential part of the University's mission.

3. Authorisation

Access to central IT facilities administered by DIT requires individual registration through which each user is given a personal userid and password. Some services, such as external access and access to management information systems require additional registration and authorisation. Details are available from the DIT Service Desk.

Authorisation to use specific systems may be adjusted or withdrawn in the event of changes in circumstances, such as contractual changes of an employee, course changes by a student, or overloading of a system. You will, however, be notified of the details of any such changes.

Unauthorised access may constitute an offence under the *Computer Misuse Act* (see also paragraph 8).

Authority granted to a user to access particular facilities may not be extended or transferred to any other person or persons without seeking further authorisation.

4. Passwords and security

Passwords must not be shared. If a password is divulged to another person, either accidentally or deliberately, a new secure password should be implemented as soon as is practical

5. Restricting or jeopardising system performance/access

Knowing propagation of a computer virus, worm, mail bomb or other program designed to impair IT services will be treated as a serious breach of Conditions.

Accidental propagation of a computer virus, due to a failure to take precautions against such propagation, will also be treated as a breach of Conditions. Virus protection and detection software is available from DIT. Remember that viruses may be propagated via e-mail attachments.

To avoid potential interference with system performance, users are not permitted to run services for other users on central computing systems without first seeking permission from DIT. This includes operations such as running a Web server or an IRC server.

Unnecessary experimentation with commands and programs that affects or has potential to affect system performance or accessibility will be treated as a reckless action. Running port scanning software is prohibited.

6. Connecting to the University Network

Procedures are available at www.abdn.ac.uk/dit/policy.php - see *Network Connection Policy*.

7. Confidentiality and security of data

7.1 Access to an item of software or data, does not imply the right to copy it to others.

7.2 The terms of licence agreements must be observed, however inconvenient. Every user must take reasonable precautions to satisfy himself or herself that the use of any dataset or item of software is within the terms of the relevant license agreement. Some typical restrictions are:

- The software/data may be used only for the purposes set out in the agreement and only on computer systems covered by that agreement.
Note: Use for other than educational or research purposes is usually prohibited; even departmental administrative use is prohibited in some cases; use outwith the UK may also be prohibited.
- The Copyright statement must not be removed or altered on any copies of the software.
- The software/data may not be transferred or lent to another person.
- A modified version of the software may not be incorporated in any other program without express permission from the Licensor.
- No attempt must be made to reverse engineer or decompile the software or to translate the software into another language or code.
- Only a personal, non-transferable and non-exclusive right to use a copy of the software or to the intellectual property in the software is transferred to the purchaser or user.
- All copies of software held by an individual person must be returned to the University when that person ceases to be a legitimate user or when requested to do so.

Further details of license agreements can be obtained from DIT which can sometimes negotiate relaxation of restrictions for particular purposes.

7.3 Holders of confidential data have a legal obligation to protect the integrity of that data.

Members of staff processing personal data are responsible for ensuring that this is carried out in accordance with data protection legislation. Students using such data should be adequately advised and/or supervised by staff responsible for the students' coursework or research activity.

For their part, DIT will take all reasonable steps to protect the information entrusted to their care and, if requested, DIT will advise users on appropriate additional safeguards.

8. Some (but not all) applicable laws

- *Copyright, Designs and Patents Act 1988, Copyright (Computer Programs) Regulations Act 1992*
- *Computer Misuse Act 1990, Telecommunications Act 1984, Data Protection Acts 1984 and 1998*
- *Criminal Justice and Public Order Act 1994*

The *Copyright, Designs and Patent Act 1988* explicitly recognises a computer program as a *literary work* for the purposes of affording copyright protection. Generally, only the copyright holder has the right to copy, or to permit another person to copy, software. Every user must comply with the requirements of this Act and of the *Copyright (Computer Programs) Regulations Act 1992* which amend it and, in particular, must not copy software except to the extent (if any) permitted in the relevant licence agreement. Copyright subsists for the lifetime of the author plus 70 years.

The *Computer Misuse Act 1990* creates three criminal offences in relation to computer misuse:

- 1. Unauthorised access to computer material.** This includes a *remote* hacker attempting to gain unauthorised access or a user with limited authorisation who knowingly exceeds that authority. The hacking need not be directed at a particular computer, program or data. For example, without proper authority, it is unlawful:
 - to use another person's userid and password in order to access a computer or use data or a program;
 - to alter, delete, copy or move a program or data, or simply to output a program or data;
 - to lay a trap to obtain a password.
- 2. Unauthorised access to a computer system** with intent to commit or facilitate the commission of a further offence. This covers a range of situations, e.g. where a person gains unauthorised access to one computer system in order to facilitate access to another system.
- 3. Unauthorised modification of computer material.** This offence is designed to cover deliberate erasure or corruption of programs or data, including the introduction of viruses or worms, modifying or destroying a system file or another user's file.

Processing of personal data must be carried out in accordance with the *Data Protection Acts (1984 & 1998)* and the University's registration under these acts. The University has a special set of guidelines to help with this which may be found on the Web at: www.abdn.ac.uk/dataprotection/

9. Other relevant Codes of Practice/guidelines

- *Code of Practice for the Publishing of Information in Electronic Format* - this is on the Web at www.abdn.ac.uk/dit/policy.php. It applies to e-mail and news groups, as well as WWW publishing.
- *Data protection* guidelines - see note 8 above.
- *E-mail etiquette* - see www.abdn.ac.uk/outlook/etiquette.shtml

10. Use of external facilities

The *Acceptable Use Policy of JANET* is available on the World Wide Web at www.ja.net/services/publications/policy/aup.html

11. Access to user files, data and e-mail

UK legislation allows the University to intercept without consent for purposes such as recording evidence of transactions, performance monitoring, and detecting crime or unauthorised use. Further details on this are available on the Web at www.abdn.ac.uk/dit/policy.php.

In the case of IT facilities administered by DIT and any system connected to the University network, authorisation to access or require access to data and files or to suspend user authorisation rests with the Director of Information Technology.

12. Disciplinary procedures

Disciplinary procedures for staff and students are available on the Web at www.abdn.ac.uk/hr/policies.shtml and www.abdn.ac.uk/registry/quality/appendix5x15.pdf, respectively.

13. Leaving the University

Once you leave the University, you no longer have any right to access IT facilities, unless you have specific permission to do so. Permission for a limited period of continued access will normally be granted to research students finishing off their thesis, or staff transferring to another University. Such permission should be sought *before* you leave the University.

Research students must obtain their supervisor's permission before copying, retaining or deleting any files relating to their research data and studies. In the event of a dispute between a student and a supervisor, the question will be referred to the Convenor of the University Research Committee for a decision.

Other students may copy, retain or delete files created by themselves during their course of studies unless instructed otherwise.

All files created by an employee in the course of their University duties may not be copied or deleted without express permission.