



The Open University Student Computing Code of Conduct

- 1 Our computing resources are provided for educational, training and research purposes. You must not use them for any business or significant personal purposes.
- 2 Before you use some of our computing facilities, you may have to get authorisation by following our registration procedure. During registration, you may be given a username, preferred name and password to use the computing facilities. Your preferred name can be changed but must remain a true representation of your name as held on University central records.
- 3 You are responsible for all activities carried out under your username. You must not give your password to anyone else or store it on another computer system. While you are logged into our system with your own identifier, you should not leave your computer unless you can be sure that nobody else can use it while you are away, for example, you have a password-protected screen saver or you can lock the door behind you.
- 4 Your password must be in line with accepted good practice. Visit www.open.ac.uk/students/help for advice on suitable passwords.
- 5 No-one must jeopardise the integrity, performance or reliability of computers, networks, software and other stored information that belong to us. In this code, 'software' includes programs, routines, procedures and their associated documentation which can be used on a computer system, including personal computers and workstations. The integrity of our computer systems is jeopardised if you do not take enough precautions against malicious software (for example, computer virus programs). You should be aware that email attachments may carry viruses, so if you are in any doubt, you must not open the email if you do not have up-to-date anti-virus software.
- 6 Just because you are able to do something does not mean that it is acceptable. Existing standards of behaviour apply to computer-based information technology just as they would apply to more traditional media. Examining all the files on your colleague's hard disk is the same as examining their filing cabinet, and trying to find unprotected files on a multi-user system falls into a similar category. While it is possible to send offensive, obscene or abusive information on the computer, this behaviour is not acceptable. For specific services, we may provide more detailed guidelines.
- 7 You must not interfere with, or try to interfere with, information that belongs to another user. Similarly, no user must make unauthorised copies of information belonging to another user.
- 8 In exceptional circumstances, we may have to use your email, voice mail or other files to carry out our work or meet our legal obligations. Each action must be authorised by a senior University officer and the user must be told. You should not assume that any online or phone conversations you have with us (or with other members of the University using our equipment) are private, because we record these in case there is a complaint or a legal inquiry. We will not eavesdrop or read these back unless we have a good reason. You should be aware that we record the internet services that are used on our network. In exceptional circumstances,

information that is being transferred may be analysed on the authorisation of a senior officer of the University. University staff may need to access your email in order to investigate technical problems, in response to a complaint or through a subject access request. Email that is clearly personal may not be opened unless there is good reason to believe that a criminal offence is being committed or a University regulation is being broken. Any email clearly marked as "personal" will not be provided to the University's Data Protection Officer(s) in response to a subject access request. Messages sent to public areas cannot be regarded as private personal information.

Staff who are authorised to reveal data (in storage or transit) must follow strict ethical standards as a condition of their employment. They must only reveal data that is absolutely necessary.

- 9 Any software or hard copy of data or information which you have not provided or generated, and which may become available by using computing or communications resources, must not be copied or used without our permission or the permission of the software or information provider.
- 10 You must not break any copyright in documentation or software (or both). The Copyright, Designs and Patents Act 1998 gives copyright owners the right to bring civil proceedings if anyone breaks a copyright, and makes it a criminal offence to break certain copyrights.
- 11 You must not use any University computing or network resources to use or publish material that is obscene, libellous or defamatory, or breaks our code of practice concerning harassment. You are personally responsible for your contributions to any OU computing system.
- 12 Software or information we have provided may only be used for educational purposes unless agreed otherwise. You agree to follow all the licensing agreements for software that we have entered into.
- 13 You agree to follow the conditions of the Computer Misuse Act (1990), the Criminal Justice and Public Order Act 1994, the Data Protection Act (1998) and other relevant Acts.
- 14 You must not do anything that damages our reputation.
- 15 You may only use approved University links to other computing facilities which you are authorised to use. When using external facilities, you must also follow their rules or code of conduct.
- 16 People who break this code of conduct may have to face our disciplinary or criminal procedures (or both).

Revised May 2005

Approved by the University Secretary