Cambridge University Engineering Department

General Rules and Guidelines Governing the Use of Computers

These notes are derived from http://www-h.eng.cam.ac.uk/help/rules/general.html, they summarise the main points but for full details see http://www-h.eng.cam.ac.uk/help/rules. Notices may also from time to time be issued in the Departmental Bulletin, see http://intranet.eng.cam.ac.uk, or via teaching system notices available at http://www.eng.cam.ac.uk/info/sysnews. Users are expected to make themselves aware of these notices.

Users should be aware that private data (including email) may sometimes be included in the process of investigating malfunction or the suspected misuse of computer systems or the network. The arrangements for such investigations are detailed in http://www-h.eng.cam.ac.uk/help/rules/admin.html. Personal data about all members of the Department (including students) is held in the Department's databases, in accordance with the Data Protection Act, as detailed in http://www3.eng.cam.ac.uk/admin/dpa .

User Identifiers and Accounts

- User identifiers are issued for use by a single named individual. All users of systems attached to the Departmental network must be registered on the central Departmental computer system. See the Helpdesk to register.
- You must not log in using another individual's login name, or allow any other person to access facilities using your login name. You should therefore not leave unattended logins on publicly accessible systems, including those in the DPO (where it is also antisocial in preventing others using the terminal).
- You must set a secure login password (http://www-h.eng.cam.ac.uk/help/sjm/DPO_system/password.html) and keep it secret. The choice of a secure password is essential both to the security of your own account and potentially to those of others; as many means of "hacking" systems require the hacker to have an account on the system to which they can login.

Responsible Use of Computing Facilities

- Accounts on the Engineering Systems are issued primarily for academic work. A small amount of recreational use is permitted but this must not interfere with academic use of the system or annoy or upset other users, e.g. by causing noise or displaying pornographic images.
- The Teaching System is a shared Departmental facility and must be used responsibly, allowing fair access to all those needing to use it. Access is restricted during teaching and there are a separate set of *guidelines* covering this, see http://www-h.eng.cam.ac.uk/help/DPO_system/access.html. At all times long running jobs must be run using the appropriate facilities see http://www-h.eng.cam.ac.uk/help/unix/LongRunningPrograms. For security and other reasons, server processes (e.g. IRC daemons) must not be left running on the system.
- Information belonging to other users is confidential. You must not read, access or modify any file not owned by you without the explicit permission of the owner. On the CUED Teaching System user files are, by default, protected from read or write access by others. Even when a file is not protected in this way, (i.e. read or write access by others is allowed), it should NOT be assumed that permission to access the file is granted.

Responsible Use of The Network

- Users must not misuse networking facilities, eg by attempting to access remote computer systems without proper authorisation, and the network must not be used for any illegal purposes (see Legal and Related Responsibilities section).
- Systems attached to the Department's network and their users must be registered, as must any other external connections which could provide independent access to the network (eg ADSL, VPNs, modems). Proper care must be taken to ensure their security and that of the network as a whole. See the `http://www-h.eng.cam.ac.uk/help/rules/network.html` for further details.
- The Department is charged on a volume basis for network traffic external to the University. Also, whilst the Department aims to provide a modern high bandwidth network, no network is immune to congestion caused by very high traffic levels. Users must therefore be careful not generate large volumes of traffic unnecessarily or for purposes other than the Department's academic work. Streamed video for more than a few minutes and transfers of large amounts of data are likely to be significant in this respect.
- Users must not attempt to hide their identity or impersonate someone else. Email and other communications must not be abusive, intimidating, harassing or misleading. The sending of bulk unsolicited email is not permitted and you should not retaliate if you get junk email. See the *rules on email* at `http://www-h.eng.cam.ac.uk/help/rules/mail.html` for further details.
- Web pages must conform to Departmental guidelines and any Web server on the Department's network must have the approval of the appropriate Divisional Web Administrator. See `http://www-h.eng.cam.ac.uk/help/rules/www.html` for further details.

Legal and Related Responsibilities

- Users have a general obligation to be aware of and abide by all legislation applicable to their use of computers. This section covers the most commonly applicable areas.
- The permission of the copyright holder must be obtained before copying or distributing any copyright material whether software, music or video. The page on *copyright* at `http://www-h.eng.cam.ac.uk/help/rules/copyright.html`, provides further details and a list of programs whose use infringes copyright and which must not be used on any system in the Department.
- All software must be used correctly in accordance with any licensing conditions. For guidance on your obligations in this area see `http://www-h.eng.cam.ac.uk/help/rules/licence.html`
- The use of Departmental systems to view, store or distribute pornographic material is contrary to the Department's rules.
- Storage and use of data about identifiable individuals is regulated by the *Data Protection Acts* 1984 and 1998. If Departmental computing facilities are used for such purposes, the use must be registered. For further information see the Department's Data Protection Officer's (`dpa-officer@eng.cam.ac.uk`) pages at `http://www3.eng.cam.ac.uk/admin/dpa/`

The Rules

- All users are required to sign a declaration agreeing to abide by the Information Services Committee Rules. Note that serious misuse of facilities may be dealt with by a Disciplinary Panel of Syndicate Members, which has power to fine or suspend users guilty of misconduct. Minor misuse of the Department's systems may be punished by a system of *fixed penalty fines,* see `http://www-h.eng.cam.ac.uk/help/rules/fines.html`
- The University Computing Service issue further *guidelines* on the interpretation of the ISC Rules, see `http://www.uis.cam.ac.uk/isc/rules-and-guidelines/guidelines`

Rules Made by the Information Services Committee

The most recent version of the rules made by the Information Services Committee (ISC) under the provisions of Regulation 5(g) for the ISC for the use of University and College information technology facilities is set out below. It should be noted that, although that regulation limits any fine to the sum of £175, offenders may also be required to reimburse costs, which may amount to a much larger sum.

The term IT facilities shall mean the facilities of University Information Services, and all other information technology facilities provided by the University, and any in College institutions designated by the appropriate College authority concerned as facilities to which these rules shall apply.

IT facilities are provided for use only in accordance with the aims of the University and the Colleges as promulgated from time to time, unless stated otherwise by the appropriate Authorized Officer.

1. No person shall use IT facilities, or allow them to be used by others, without due authorization given by the ISC or by the appropriate Authorized Officer, who may impose conditions of use to ensure efficient operation.

2. By means of published documentation an Authorized Officer may designate an IT facility as authorized for use by specified classes of persons and for specified purposes. In the case of facilities not so designated, resources are allocated individually; every such allocation of IT resources shall be used only for the designated purpose and only by the person to whom the allocation was made. Use shall not be made of IT resources allocated to another person or group of persons unless such use has been specifically authorized by the ISC or by the appropriate Authorized Officer.

3. No person shall by any wilful, deliberate, reckless, unlawful act, or omission interfere with the work of another user or jeopardize the integrity of data networks, computing equipment, systems programs, or other stored information.

4. All persons authorized to use IT facilities shall be expected to treat as privileged any information which may become available to them through the use of such facilities and which is not obviously 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 appropriate person or body.

5. In the case of any information which is designated in a Notice issued by or on behalf of the ISC as proprietary or otherwise confidential, every person using IT facilities shall be required:

(a) to observe any instructions that may be issued specifying ways in which the information may be used;

(b) not to copy, modify, disseminate, or make use of it in any way not specified in those instructions, without first obtaining permission from the appropriate Authorized Officer.

6. No person shall use IT facilities to hold or process personal data except in accordance with the provisions of relevant legislation, including the Data Protection Act 1998. Any person wishing to use IT facilities for such a purpose shall be required to inform the Authorized Officer in advance and to comply with any restrictions that may be imposed concerning the manner in which the data may be held or the processing carried out.

7. No person shall use IT facilities for private financial gain or for commercial purposes, including consultancy or any other work outside the scope of official duties or functions for the time being, without specific authorization to do so.

8. Any person who misuses IT facilities or who uses IT facilities for private financial gain or for commercial purposes, with or without specific authorization to do so, may be charged with the cost of such use or misuse at a rate determined from time to time by the appropriate Authorized Officer. If any person who has been so charged with the cost of IT resources fails to make reimbursement, any authorization to use IT facilities shall be suspended automatically until reimbursement is made in full, and the matter shall be reported by the ISC to the appropriate University or College financial authority.

9. No person shall use IT facilities for unlawful activities.

10. Any person believed to be in breach of one or more of these rules shall be reported by the Authorized Officer to the ISC who may at their discretion, after considering the Officer's report and any other relevant matters, impose a penalty or penalties in accordance with Regulation 5(g) for the ISC. The ISC may also recommend to the appropriate University or College authority that proceedings be initiated under either or both of the University and College disciplinary procedures and any appropriate legislation.

Last updated 2014.