University of Bristol

Regulations for the use of computing facilities

These Regulations should be read in conjunction with the University's Code of Conduct for the Use of Computing Facilities and other related guidelines available from the Computing Service or on the Information Services website at
http://www.bris.ac.uk/is/selfhelp/documentation/code-g1/code-g1.html

1 Scope

1.1 Users
These regulations apply to everyone using the University's computing facilities. In particular they apply to staff and students at the University, and to people outside the University who have been given permission to use the University's facilities.

1.2 Permission to use the University's computing facilities
External users normally require explicit written permission from the Assistant Director of Information Services (Information Systems and Computing) to use the University's computing facilities, even where no registration is needed.

External users registered to use Library facilities will not need permission to use the Library catalogue, but may be required to seek permission to use other computing facilities in libraries.

Users should be aware that the University retains the right to monitor messages and materials sent over its network to check that the user is not in breach of these regulations (see Policy for the Investigation of Computers).

1.3 Facilities
The computing facilities covered by these regulations include all computers located in the University, including multi-user hosts, workstations and personal computers, together with the software and data stored on them. The regulations also cover all computing carried out on a computer connected to the University network, whether or not this involves the use of a University-based or University-owned computer.

These regulations do not cover any computing facilities external to the University. Use of other facilities and networks is subject to the regulations appropriate to each of them. In particular, use of the JANET network is subject to the JANET Acceptable Use Policy, a copy of which can be found at http://www.ja.net/

2 Relevant legislation

Users must comply with all UK legislation relating to the use of information, computers and networks.

2.1 Computer misuse
Users must not:

(a) access (or display any information which permits another to access) computer material without authorisation for perpetration of any criminal offence;
(b) alter (or display any information which permits another to alter) data, programs, files,

electronic mail or any other computer material belonging to another user without the other user's permission;
(c) use (or display any information which permits another to use) a computer to access any program or information which they are not authorised to access/use.

2.2 Copyright and rights in software
The University expressly forbids the illegal copying of software by staff or students. All users must respect rights in proprietary software and other on-line information. Users may not copy proprietary data from any systems without permission, nor install proprietary software on systems not covered by an appropriate licence.

Heads of department are responsible for all software installed on the computers in their departments. The University may carry out audits from time to time to ensure all software is legal.

Many software packages in the University are licensed only for educational use, and must not be used for commercial purposes unless a full licence is obtained.

Disciplinary action will be taken against staff or students who knowingly make, acquire or use unauthorised copies of computer software.

Users may not upload or download information through the University's computing facilities which is not authorised by the copyright owner or permitted by law. Users must not make, transmit or store electronic copies of copyright material on the University's computing facilities without the permission of the owner. A serious breach of copyright could result in disciplinary action. (Further information can be obtained at http://www.bris.ac.uk/Depts/Secretary/guide00.htm).

2.3 Data Protection
Any work involving processing, storing or recording personal data (i.e. information on an identifiable individual) is subject to the Data Protection Act 1998. It is the user's responsibility to ensure that personal data is collected in accordance with the Act. Personal data must be fairly obtained, securely stored and access only given to those who need it. (Further information can be found at http://www.bris.ac.uk/Depts/Secretary/datapro.htm).

Users must:

(a) in cases of doubt, contact the University's Data Protection Officer before conducting an activity which involves the collection, storage or display of personal data, to find out whether the proposed use of personal data complies with the University's notification;
(b) ensure that all records containing personal data are accurate and up-to-date. You should not keep personal data records for longer than is necessary;
(c) carefully review any disclosures of personal data, both within and, particularly, outside the EEA;
(d) ensure that all information stored on a computer is professionally removed when the computer is passed to another user, sold or otherwise disposed of, in accordance with the University’s policy on the disposal of computer equipment (http://www.bris.ac.uk/is/services/computers/general/disposal)
(e) ensure that personal data is not taken home or stored on a home computer.

Failure to comply with the terms of the Data Protection Act may result in both criminal charges and civil actions for compensation. A serious breach of the Act could constitute a serious disciplinary offence and will result in internal disciplinary action.

2.4 Offensive or defamatory material

All information that is made available on-line to other people, either by electronic mail or in publicly accessible file space (for example in Usenet news or on the World Wide Web) must not be discriminatory, pornographic, homophobic, excessively violent, obscene, libellous, blasphemous, seditious, incite racial hatred, or in any way break any law pertaining to published material. Users must not access, store, display, receive, download or transmit offensive or obscene material.

In addition, users must not publish any information on-line which will cause offence or needless anxiety to people who might normally be expected to read it, or make any defamatory statement. A defamatory statement could be contained in articles, letters, emails and visual images. Users must not use threatening, abusive or otherwise objectionable language in either public or private messages.

The University will regard the publication or possession of offensive or obscene material as a serious disciplinary matter and, with regard to obscene materials, will not hesitate to inform the police. In the unlikely event that there is a genuine academic need for accessing offensive or defamatory material, the University must be made aware of this and prior permission must be granted from the Assistant Director of Information Services (Information Systems and Computing).

2.5 Discrimination

Users must not use the University's computing facilities to place, disseminate or receive materials which discriminate or encourage discrimination on the grounds of gender, sexual orientation, disability, race or ethnic origin.

2.6 Official Secrets Acts 1911 - 1989

The Official Secrets Acts 1911-1989 establish severe criminal penalties for any person who discloses any material which relates to security, intelligence, defence or international relations and which has come into that person's possession through an authorised or unauthorised disclosure by a Crown Servant or Government contractor.

Users must ensure that any such material is securely stored and avoid displaying it on the University's computing facilities.

3 Use of University’s computing facilities

3.1 Access

Users must not provide access to any of the University's computing facilities to those not rightfully due such access. Any activity carried out by a user for any fee or other consideration is in contravention of these regulations unless prior approval has been obtained from the Assistant Director of Information Services (Information Systems and Computing) or, for departmental facilities, the head of department. The University's computing facilities must not be used for placing or distributing advertisements relating to any course of business other than those promoting the University's teaching and research activities or its own trading operations.

3.2 Identification
Users may not use a personal identifier or passwords allocated to another user, nor pass their own personal identifier or password to another person. Users may not pass themselves off as another person when sending electronic mail, posting to Usenet or making information available on-line in any other way. No device attached to the University's network may be configured with any addresses other than those issued to it or authorised for it by appropriate staff in the University's Information Services Department.

3.3 Compliance with Policies, Codes and Regulations
Users must comply with the relevant Acceptable Use Policies associated with all computer networks of which use is made. If computing facilities at another site are employed, users must comply with the regulations and codes governing that site.

3.4 Responsible use of the University's computing facilities
Computing facilities are provided for use by staff in the course of their employment and by students in the course of their education. While other incidental and occasional use may be permitted such use must not interfere with the employee's work or the student's study. Any abuse of such permission will be treated as a contravention of these regulations.

The following will also be treated as contravening these regulations:

(a) any action that would impair the function or security of the University's computer network;
(b) any action that denies another network user access to network services;
(c) connecting any device to the University's network without first registering the device with a Departmental Network Representative;
(d) attempts to penetrate security and/or privacy of other users' files;
(e) any use of the University's computing facilities that brings the University into disrepute;
(f) making, storing or transferring unlicensed copies of any copyright or trademark work including computer programs;
(g) setting up web servers, or placing web pages on any of the University's computing equipment, other than that provided for the purpose by the University;
(h) sending bulk e-mail material unrelated to the legitimate educational business of the University, including the transmission of bulk e-mail advertising (spamming);
(i) sending unsolicited e-mail messages requesting other users, at the University or elsewhere, to continue forwarding such e-mail messages to others, where those e-mail messages have no educational or informational purpose (chain e-mails);
(j) sending e-mails which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing);
(k) sending or receiving material which is illegal under UK law, which may give rise to legal action against the user and/or the University, or which contravenes any of the University's regulations or guidelines.

Many computers in the University provide access to computer networks that enable users not only to connect to computers at other educational establishments, but also to connect to computers at many sites not related to the education sector. The ability to connect to a computer does not automatically give users the authority to use it. If the system displays a message that explicitly states that users do not need to be authorised to use it, they may use the system. If there is no explicit message, users should not attempt to use the system. System administrators are obliged to inform the Information Services of any detected or suspected misuse of the systems for which they are responsible.

4 Penalties

4.1 Withdrawal of facilities

If a user is in breach of any of these regulations, the Assistant Director of Information Services (Information Systems and Computing) may withdraw or restrict his or her use of computing facilities, following consultation where appropriate with the user's head of department or dean of faculty.

4.2 Disciplinary action

Any breach of the regulations may be reported to the Vice-Chancellor to be dealt with under the University's disciplinary procedures. Information Services may request that a user be charged for extra work or expenses that have arisen as the result of computer misuse.

4.3 Breaches of the law

Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach will be reported to the relevant authorities within that jurisdiction.

Revised version approved by Council 22 March 2002.

http://www.bristol.ac.uk/Depts/Secretary/regscomp.htm

Rules and Regulations for Students 2005/06