

Information Systems Regulations

1 Introduction

Your use of College IT resources is subject to the terms outlined below, but there is also an expectation that you will adopt a common-sense approach to their use. This is as much concerned with courtesy, consideration and social obligations as it is with your adherence to these regulations.

The College's connection to the Internet is provided by JANET (Joint Academic Network), the body which supports the communication requirements of the UK education and research community. Accordingly, you must also abide by the JANET Acceptable Use Policy (see <http://www.ja.net/services/publications/policy/aup.pdf>).

2 Allowed Users of College IT Resources

College IT resources are for registered users only. All staff and students of the College may be registered as users. Any other person may be registered as a user at the discretion of the Information Systems Manager and may be subject to such charges or additional conditions as the Information Systems Manager may determine.

3 Inappropriate Use of College IT Resources

The acts below are considered inappropriate and, if committed, could lead to disciplinary action being taken against you. In addition, some of the actions listed, for example accessing pornographic content via the Internet, could lead to criminal prosecution.

You must not

- use College IT resources to offend or harass
- send sexist/defamatory/indecent/obscene/pornographic/violent/offensive material via College IT resources including e-mail
- access sexist/defamatory/indecent/obscene/pornographic/violent/offensive material via the Internet
- use College IT resources for personal consultancy or other private or commercial work
- participate in distributed file-sharing networks (e.g. using peer to peer software)
- attempt to access any IT service you have not been given permission to
- cause any form of deliberate damage or disruption to services to College IT resources which includes equipment and software, or to any of the rooms that contain the equipment
- use College IT resources to communicate personal opinions on College related or other matters to multiple addresses/grouped email addresses

The above list is not intended to be exhaustive, but is an indication of the types of act that the College considers inappropriate.

4 Personal Use of College IT Resources

- Staff

In general, you should not use College IT resources for activities unrelated to your work. Limited personal use is acceptable (e.g. during a lunch break), but you may be disciplined if you engage in personal use of IT resources when you should be attending to your duties.

- Students

In general, you should not use College IT resources for activities unrelated to your studies. Limited personal use is acceptable, but you should not prevent another student from using the IT resources for their studies.

5 The College E-mail System

When using the College e-mail system you must not

- send an e-mail message that contains defamatory comments. E-mail is a form of publication and the laws relating to defamation apply
- send an e-mail that shows the College in an unprofessional light or that could expose the College to legal liability. Messages sent using the College e-mail system have the same standing as a letter on headed paper
- send e-mails which contain offensive or obscene content
- send e-mails which discriminate or encourage discrimination on the grounds of race, ethnicity, sexual orientation, marital status, age, disability, political beliefs or religious beliefs
- send unsolicited e-mails to multiple recipients, except where it relates to the academic or administrative activities of the College
- send emails to communicate personal opinions on College related or other matters to multiple addresses/grouped email addresses

6 Monitoring of E-mail and Internet Use

Where there is reason to suspect misuse (e.g. to determine if someone is accessing pornography), the College reserves the right to monitor your use of e-mail and the Internet. Such monitoring will only be carried out on the authorisation of the College Management Team.

Information Systems Department staff can access all data held on College IT equipment or transferred over the network. Any information obtained in the course of this duty that is thought to indicate misconduct or a breach of the Information Systems Regulations will be brought to the attention of the College Management Team.

7 Security of College IT Resources

You must not

- leave a logged-in workstation unattended
- disclose your password to anyone else, unless the disclosure is necessary for the administrative function of the College. For example, to allow someone else to access your data (with your permission) while you are away
- attempt to access any College IT resources that you have not been given permission to do so

Staff must not

- allow a student to use their workstation (or that of another member of staff) without supervision

8 Integrity of College IT Resources – Backup

Regular backup copies will be made of data held on the College's network servers, but recovery of lost or damaged data cannot be guaranteed. If you choose to store data on the hard disk of your own workstation, you are responsible for the creation of regular backup copies.

9 Storage of Personal Data – Data Protection

If you use College IT resources to store personal data relating to living individuals (e.g. a database of names and addresses), you must ensure that the use and storage of the information complies with the College's registration under the Data Protection Act 1998. Personal information can only be used for the purpose it was initially collected for (with the persons consent) and should not be stored any longer than is necessary.

It is discouraged to remove personal information from College premises and upon doing so the individual is liable for its security and safe keeping.

Further guidance on this matter can be sought from the Information Systems Manager. Room: 3.45 REB, tel: 1381 (029 2039 1381) or email: IT@rwcmd.ac.uk

10 Accessing Individual Computer Accounts and Work

The College retains the right to access all College e-mail accounts, network drives and College computers to ensure continuity of College business. Members of staff with access to other people's mailboxes and personal network drives will be subject to respecting privacy. This means that neither any e-mail/ file clearly marked as "personal" should be opened, nor any e-mail/file be opened that is obviously not College business. Failure to do so may lead to disciplinary action being taken.

All e-mail received will be considered as being for College business unless specifically indicated otherwise. If a member of staff is absent for a period of one week or more and cannot be contacted, the College reserves the right to access their e-mail or set out of office replies to ensure that College business is not adversely affected. This option may also be exercised to ensure compliance with a request for information under the Freedom of Information Act or Data Protection Act.

11 Installation of Software or Hardware

You must not

- install any software or hardware on IT resources managed by the Information Systems Department, unless authorised to do so by the Information Systems Manager
- connect (either via physical cable or wireless link) equipment to the College's computer network, unless authorised to do so by the Information Systems Manager

12 Loan of College IT Equipment

Unless allocated for that purpose (e.g. laptop computers or portable USB storage devices), you must not use College IT equipment outside the College premises. Other equipment may be used outside College premises solely at the discretion of the Information Systems Manager.

13 Disciplinary Action

Any breach of these regulations may be regarded as your behaving in a manner inconsistent with the proper functioning of the College under the terms of the Staff and Student Disciplinary Codes.