Conduct (Monitoring of Email and Internet use)

1. Introduction

1.1. The University seeks to facilitate the proper and extensive use of IT in the interests of its work. This policy is intended to provide a framework for the responsible and legal use of email and internet and explains both general and specific monitoring which takes place to secure acceptable use of facilities.

1.2. All employees using the Internet and e-mail at work must comply with the University Regulations pertaining to the Use of Computing Facilities and the JANET Acceptable Use Policy (copies available on the CLS intranet).

1.3. IT resources are provided to facilitate an employee's work. Use for other purposes, such as personal e-mail or recreational use of the World Wide Web, is allowed as a benefit to staff. Such access is not a right. Any use must not interfere with the employee's duties or any one else's use of facilities for work purposes and must not, in any way, bring the University into disrepute.

1.4. While the University routinely monitors the overall patterns of e-mail and Internet usage it does not, in the normal course of events, specifically identify the use made of the facilities by any individual employee. However, a record of log-ins is maintained and may be considered in an investigation. Under the Regulations of Investigatory Powers Act 2000, email and Internet systems are subject to random monitoring and recording by or on behalf of the University. Accordingly, while the University will at all times seek to act in a fair manner, employees should be aware that there can be no legitimate expectation of privacy when using the University's e-mail and Internet facilities.

1.5. Specific monitoring of the use of facilities both from examination of files held on the server and files held on an individual hard drive may be undertaken in investigating specific allegations of a breach of conduct under the University's disciplinary procedures.

2. Definitions of Unacceptable Use

2.1. Unacceptable use of university computers and network resources are:

- the viewing, retention or distribution of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law
- causing annoyance, inconvenience or needless anxiety to others, as specified in the JANET Acceptable Use Policy
- defamation
- intellectual property rights infringements
- unsolicited advertising ("spamming")
- attempts to break into or damage computer systems or data held thereon
- the distribution or storage of pirated software
- non work activities which generate heavy network traffic, especially those which interfere with others' legitimate use of computing facilities or incur a financial cost

3. Blocking and monitoring internet access

3.1. The University maintains a policy of blocking access to web sites containing pornographic or other material that could be deemed offensive. All such access to these sites is logged and monitored. If monitoring reveals possible evidence of criminal activity, or a repeated breach of the computing regulations or JANET acceptable use policy by attempting to access these sites or similar sites a disciplinary investigation will be instigated, and the police may be notified (where relevant).

3.2. Through general monitoring of internet access the Computer and Library Services regularly update a list of internet pornography sites that are blocked to access. If an employee attempts to access a blocked site the employee will be notified automatically.

3.3. If multiple attempts are made to access blocked sites within 24 hours a report is forwarded to CLS, identifying what blocked sites and other non-blocked sites were accessed. The records will be reviewed by the authorised CLS staff member and where the log evidence suggests inappropriate use the name of the user will be extracted from the logs. This information, with proxy server log records, is forwarded to HR who will advise the line manager on appropriate investigation and access under the University's disciplinary procedures.

3.4. In the rare event that an individual requires access to blocked sites as part of a teaching or research proposal clearance must be obtained from the School and University Ethics Committee. Such approval should be forwarded to the Head of C+IT and should provide specific timescales where access is approved.

4. Other Investigations

4.1. Where specific allegations are received relating to the conduct of the employee the University reserves the right to check computer files held on backup files and on hard disks. In such cases the individual will be informed of the allegations and the nature and scope of the investigation being undertaken.

4.2. On rare occasions the police may request information regarding an individual's computer records. In such cases access to information will be governed by legal process.

5. Other Access Requirements or Restrictions

5.1. The use of facilities for commercial work may only be made in accordance with the Guidelines for Undertaking External Work, available in the Academic Staff Handbook.

5.2. Individuals should not assume that the University's system is secure. If employees use the University Internet or email access to carry out on-line transactions the University takes no responsibility for any part of the transaction and is not liable for any failure of security that might occur as a result of the transaction.

5.3. Employees should not use another user's identification or allow another person to use their reference. Employees are responsible for the security of their own password and should they divulge the password to allow someone access under their own reference they will be accountable for the use of their account by the other person.

5.4. Where an employee is absent from work for a period of time and has been unable to make file share arrangements the Dean or Director may authorise access to an employee's computer to access work related files and email.