Conditions of Use

The following conditions of use are applicable to all usage of computers and networks at City University including office based and stand-alone systems.

It should be noted that these conditions form part of the University's conditions of employment and student regulations; breach of these regulations, particularly in relation to Data Protection and obscenity, may lead to disciplinary action. The more serious breaches may be considered under gross misconduct.

All users should be aware that by registering with us you have agreed to abide by these Computing Services "Conditions of Use" and the JANET "Acceptable Use Policy". These conditions are available online and you would do well to review them from time to time. Remember that password security is key to ensuring that your account is not misused. Take care of your password - do not share it or email it to anyone and avoid writing it down.

Resource Usage

Facilities provided by the University are intended to be used in furtherance of the aims and objectives of the University. A reasonable amount of personal use is permissible - even expected, but:

- Priority - especially at peak periods - must be given for the intended use;
- Networks - specifically including JANET through which all our internet traffic passes - may have their own Acceptable Use Policies which must be complied with;
- Licence conditions on some software or data may limit the nature of usage;
- Work of a commercial nature, or for reward, and including web sites for external organisations requires prior written permission;
- The provision of any service to non-members of the University also requires such permission;
- The use of another user's username - with or without their permission - is forbidden;
- Sharing of a personal username and password on the University system or otherwise permitting the use of a personal account by another, except with the explicit written agreement of the Director of Computing Services is strictly forbidden. It is considered misuse by both lender and borrower.
- A number of external resources are accessible by users of the University's computing systems and networks. There are specific conditions of use which govern the use of these resources.

Potential for harm

Certain activities that are not, of themselves, necessarily illegal or damaging are restricted because they may pose a risk of damage, of expensive consequences, or of harming the reputation of the University. Specific rules of this nature include:

- The storage or publication of information (including on web sites) intended to breach copyright or security is forbidden. Some copyright material may be used for teaching - see here for guidelines;
- Do not eat, drink or smoke in the workstation rooms;
- Keep mobile phones switched off at all times in the workstation rooms;
- The unauthorised use of network monitoring software is forbidden;
- Care should be taken not to imply that a personal statement describes University policy;
- Avoid defamatory statements, especially in "public" messages (web pages, newsgroups, bulletin boards, and mailing lists).

Investigation and Enforcement

Certain activities on the network and centrally provided systems are routinely logged and/or automatically monitored. These include:

- Usage of workstations
- Access to web pages
- Access to software
- Volume of data transfers
- Quantity of email.

In the majority of cases, the primary purpose of such logging is for fault investigation and capacity planning, anomalies may prompt investigation of possible breaches of the Conditions of Use and the information is available when evidence of possible misuse is needed.

You are advised that Computing Services regularly scans both the University web cache for obscene material as part of the Policy on Obscene material and the network to detect any vulnerable shared directories as part of the Policy on Open Shares.

When required further information may be collected - this is normally only performed in response to an investigation prompted by a specific complaint. Such a complaint may have been from the managers of remote sites and networks, from users, from the police, or as a result of an investigation prompted by an anomaly in routine monitoring. In these cases, where not forbidden by law, Computing Services reserves the right to:

- Inspect network traffic between a user's machine and any other address(es)
- Inspect - possibly via an automated search - the content of files held on any system managed by Computing Services and on any system - even privately owned - that is, or has recently been, connected to the campus network.
- Inspect email, both incoming and outgoing. **Automated filters are installed to intercept the transmission of email** to remove viruses and identify potential spam email. Further restrictions may be employed in the event of warnings about harmful software (eg viruses and worms) or security problems being received.
- Cut off access (either by disabling logins or by disconnecting from the network) where it is considered advisable to prevent further misuse.

The department may also examine any University owned computer for unlicensed software and test the security of any computer connected to the University network.

Except where it provides evidence of a breach of these conditions, of serious criminal activity, or of significant costs to the University, information acquired during any monitoring will be kept strictly confidential to those directly involved in the investigation. In the case of serious criminal activity the information will be made available to the police.

Serious breaches of these conditions will be handled by the University Disciplinary Procedures; less serious cases by summary action by a senior member of Computing Services (in this case the alleged offender may insist on the use of the University Disciplinary Procedures as an alternative). When summary action is taken, the punishment is normally a suspension of permission to use the computing facilities and network.

Regulation of Investigatory Powers Act 2000

The University is required under the Regulation of Investigatory Powers Act (2000) to being the following notice to the attention of all its users:

As required by UK legislation, Computing Services draws to the attention of all users of the University's data network the fact that their communications may be intercepted as permitted by legislation. The legislation allows the University to intercept without consent, for purposes such as recording evidence of transactions, ensuring regulatory compliance, and detecting crime or unauthorised use. The University does not need to gain consent before intercepting for these purposes, although staff and students of the University should be advised that interceptions may take place.

This is not a change of practise; staff within Computing Services have the authority to carry out certain monitoring activities in order to ensure the correct operation of the network and related systems. This does not imply that all communications are monitored but serves to advise all users that they may be for the purposes outlined above.

It should be noted that Computing Services is acting on the University's behalf as the regulatory authority in this instance. Any other monitoring of the network is expressly forbidden by the Network Code of Conduct.

Policy on open shares

Microsoft Windows operating systems allow the user to set up directories so that they can be shared with other Windows users. The guidance within the Windows Help system does not make explicit reference to securing these files and as a consequence, the directories are often left entirely open and visible to other network users. The data contained in these shared areas is available to anyone on the University network. The use of these open shares is bad practice, particularly where personal data is being stored. Indeed, storing personal data in these shares contravenes the data protection act and renders the University open to prosecution under the act.

Computing Services recommends that networked storage should be used whenever it is necessary to share data within a work group, or across a work group. Such networked storage can be obtained by contacting the Response Centre. If you are not sure whether you have shared data on your PC, you should also contact the Response Centre where a member of Computing Services will be able to help you check your computer.

A number of open shares were discovered in an initial sweep of the University network; these have now been closed. Computing Services continues to scan the network for open shares in the interest of maintaining the integrity of the University's data. In future any discovered shares that contain personal data will be treated very seriously and may lead to disciplinary action.

Policy on obscene material

The University, in response to a JISC paper on internet law, has derived a policy on obscene material. The policy, which has been approved by both Council and Senate, is underpinned by the following principles:

- The University does not seek to lay down codes of moral behaviour in this area; however, it is bound by the law, by the conditions of use of the JANET network, and may be subject to HEFCE sanctions if it does not take seriously the JISC guidance.
- Using the University's network to send or receive obscene material is a breach by the user of conditions of use and additionally may render the University liable to criminal proceedings as a distributor of such material. The University must therefore institute a pro-active policy to deter such misuse of facilities.
- It is important to distinguish different kinds of offence. Leaving child pornography aside, the act of viewing obscene material on the internet is not a criminal offence, though it contravenes conditions of use. Any disciplinary consequences should

therefore be proportionate and should follow informal warning, initially from the Director for Information rather than via the Head of Department.

- By contrast, the distribution of obscene material (including the circulation of it to another user) is capable of being a criminal offence and should be dealt with under the disciplinary procedures, which provide for discretion in the matter of report to the Police.
- Offences involving child pornography should be reported to the Police in all cases.

Computing Services will selectively monitor all incoming internet traffic by occasionally scanning the University web cache for obscene material. The scan will look for internet addresses listed on selected link sites devoted to definitely obscene material. When a user is found to have made use of such an address, his or her internet traffic will be examined in detail to see whether the usage is part of a systematic pattern of misuse. No adverse action will be taken if the misuse is not systematic since it is recognised that occasional calls to sites that prove to contain obscene material can readily be made inadvertently

Network Code of Conduct

The Data Network at City University is a University resource which is installed and managed on behalf of users by Computing Services. Computing Services reserves the right to withdraw from users permission to gain access to the network and the facilities thereon in the event of a breach of any of the following conditions of the Code of Conduct. Disciplinary proceedings may also be initiated against users in respect of any breach of the Code.

1. Prior permission must be sought from Computing Services before any attempt is made to connect equipment of any description to the network. Forms for this purpose are available from Computing Services, and they must be fully completed and signed before being returned.
2. If a connection request is approved, Computing Services will perform the installation, with the cost to be borne by the user.
3. Computing Services must be notified of all material changes including upgrades of hardware and software to permitted equipment. In particular, this includes changes to network addresses and network protocols.
4. All users are required to provide Computing Services with an email address at which they can be contacted. This address must be regularly checked for email and relevant messages responded to in a timely fashion. Computing Services will provide an email address if required.
5. All equipment must be maintained and operated at all times in such a manner that it does not interfere with or otherwise degrade the quality, performance of the network. On receipt of notification from Computing Services, any malfunctioning equipment must be immediately disconnected from the network, and reconnection may not be made until Computing Services is satisfied about the performance of the equipment.
6. When requested to by Computing Services, users must disconnect specified equipment in order for upgrades, preventative maintenance or repairs to be effected to the network.
7. No attempt should be made to examine, copy or alter data on the network that is not legitimately destined for the user. In particular, network monitoring software having the ability to observe data on the network should not be used. If such software can be shown to be essential for diagnostic purposes, then prior permission for use must be sought from Computing Services, which if granted, applies only to temporary monitoring of the users own data. Users should be aware that a breach of this condition is considered to be a serious matter, and could lead to disciplinary proceedings being taken by the University against the user. Computing Services reserves the right to use such monitoring equipment to ensure compliance with this Code of Conduct.
8. Users are required to become familiar with the regulations and requirements of the Data Protection Act and Computer Misuse Act, and must undertake not to breach the said Acts. In particular, users are not permitted to transmit onto the network obscene material or personal data about living individuals without prior permission being

granted by the University Data Protection Officer and notifying Computing Services accordingly.

9. Users must take adequate measures to ensure that any equipment connected to the network is not left at any time in such a manner that unauthorised users can gain access to either the equipment or the network. Any suspected breaches of data security or confidentiality must be reported to Computing Services immediately.
10. When accessing external sites, users should behave in a responsible manner with respect to the use of any networks and systems used. This includes - but is not limited to - avoiding times of peak loading, heavy usage for trivial purposes, and use of false identification.