Finance & IT Directorate

Monitoring and Interception of IT systems

1 Legislation

1.1 To be observed in conjunction with the IT Conditions of Use.

2 Monitoring Purpose

2.1 The University has a duty to inform its users on the extent to which monitoring and interception of information on computer systems and networks is carried out.

2.2 The Finance & IT Directorate, as the responsible agency for IT Systems and services at the University, carries out monitoring of a variety of information.

2.3 Monitoring takes place for operational purposes

- To maintain and enforce network security
- To maintain and monitor the integrity of IT systems
- To protect against viruses and SPAM
- To check for misuse of resources
- To gather usage statistics
- Network traffic for usage controls
- Telephone usage for charging purposes
- Data audit trails for systems where appropriate

2.4 Monitoring may take place for the prevention or detection of crime.

2.5 All monitoring logs will be kept for a minimum period of three months.

2.6 The Director reserves the right to examine any machine connected to the University network that is affecting IT systems or suspected to be contravening the conditions of use.

2.7 The University observes that the legislation sanctions the interception and monitoring of communications, placing limits on the powers of the organisation and the protection for the rights of individuals.

2.8 Finance and IT staff will not routinely monitor or inspect

- the contents of electronic mail folders
- the contents of any personal file store
- telephone calls except in the case of call recording for training purposes

2.9 However inspection may take place by the Director, or designated officer if

- A routine access to business communications is required when staff users are on holiday or sick
- An alleged misuse is bought to the attention of Finance and IT Directorate.
- A request is made by police as part of an enquiry.

2.10 Information gathered into logs can be found in section 4 of this document.

3 Guidelines for Inspecting User Material

In the following **user material** is defined as all user owned files and electronic mail folders. Authorization to inspect user material will be given by the Director. Where material is held on a resource under the control of a Faculty/Directorate then the appropriate authority should be the Dean of Faculty/Director (or their nominees) on the advice of the Finance and IT Directorate.

Authorised users of IT systems should be aware that personal communications, as well as communication relating to University business made via University IT systems may be monitored or intercepted whilst carrying out inspections.

3.1 All staff given privileged access to systems and networks must respect the privacy and security of the user material.

3.2 Staff responsible for the management operation or maintenance of systems and networks have the right to access user material and monitor network traffic, but only if necessary to fulfil their role.

3.3 Authorization and examination should not be carried out by the same person.

3.4 If examination proceeds in circumstances where it is not possible to get the user's permission in advance, then the user should be informed after the event.

3.5 A record should be kept of any such examination. Such a record should be available for inspection.

4 Computer System Monitoring

Information gathered by Information Services as part of the Systems, Network and Telephony Monitoring Process.

4.1 Accounting Information

Maintenance of computer accounts is automated in the case of students, based on data taken from the student records system. In the case of staff, a manual system is applied which records similar data.

4.2 Service Access Logs

Monitoring of the following is logged into separate places and can only be related to individuals by bring the information together. The following list are monitored in accordance with this policy.

- Logon to the network
- Logon to Keele servers
- Access to network drives from PCs
- Access to imap based mail servers
- Electronic mail messages posted or delivered on Keele servers
- Web pages accessed on Keele servers
- Web pages accessed on the Internet by Keele clients
- Access to file transfer (ftp) servers
- IP Traffic Monitoring
- Telephone System