1. Introduction

1.1. This document describes policy relating to how the University may monitor usage of its IT systems (including University owned Mobile Phones) and the circumstances in which it may access user information on its systems and networks that is normally private. It gives additional details about implementing the "Compliance with the University's own information security standards" policy stated in Compliance Policy (ISP-S3).

2. Institutional IT system usage monitoring and access to accounts

2.1. Students, staff and others that may use any University information system, or handle University information, must be explicitly informed and confirm acceptance of University policy relating to institutional IT system usage monitoring and access.

2.2. Students should be made aware at the point of registration, and be made aware at re-registration for each subsequent year of their course.

2.3. IT Services should make staff members aware upon their first registration on the system, and then each subsequent year of employment.

3. General monitoring and access policy


3.2. Where undertaken on behalf of the University, access and monitoring must be:

- For legitimate reasons.
- Justifiable, fair and proportionate.
- Done with the minimum possible intrusion and disruption to both the subject and any third parties involved.

3.3. Information on University owned IT equipment and networks, including mobile phones, USB sticks, tablet computers etc., may be examined on behalf of the University by authorised persons to:

- Support detection or prevention activities that are in breach of University policy.
- Comply with legislation.
- Support detection or prevention of activities that are illegal.
- Defend against attacks against its systems or data.
- Identify or investigate an operational problem or monitor for correct operation.
- Investigate suspected unauthorised access to or use of systems.
- Perform monitoring or support activities with consent of the subject.
3.4. The University has no right of access to personally owned devices; however the University does have the right to require a staff member of student to provide University information held on a privately owned device.

3.5. Monitoring of particular University information systems and access to data in user accounts may only be undertaken where authorisation has been granted by Information Assurance Services and when carried out under their direction.

3.6. **Unapproved information system monitoring or access is a breach of University regulations and may also be illegal; such activities may therefore lead to disciplinary or legal action.**

3.7. Any information collected must be handled securely, treated as confidential and only revealed to or examined by those authorised.

3.8. Any information collected must only be retained for the period deemed necessary for the specific purpose for which it was collected in line with the Data Protection Act.

3.9. Where illegality is suspected any investigation must be left to the Police and their instructions must be followed relating to identifying, seizing and preserving any digital evidence.

3.10. Where any evidence of illegality is discovered during an account access the staff members conducting the access should immediately exit the account and escalate the matter.

4. **Routine monitoring**

4.1. The University undertakes limited monitoring of the activities of students, staff and others for compliance with information security policies and other University regulations. In agreeing to abide by the University information security policies, members of the University are advised that user-specific information may be routinely monitored by authorised staff with respect to:

- Login and logout events and locations.
- System resource usage.
- Software usage.
- Software auditing to support compliance.
- Network bandwidth usage.
- Network bandwidth usage and traffic patterns.
- Power consumption.
- Detection of email spam.
- Detecting security vulnerabilities.
- Identifying and controlling security threats.
- Serving inappropriate content, which may include material which is obscene, violent, illegal, damaging to the University or otherwise in breach of University policy.

4.2. Other than automated monitoring as described in 4.3 below, routine monitoring does not include examining the contents of files and communications for any purpose which has not been previously approved as a requirement of legitimate University business.
4.3. Use of automated systems which scan user files and communications for an approved purpose is permitted.

4.4. Those with elevated access privileges, such as IT system and network administrators, are not entitled, simply by virtue of having those privileges, to examine the contents of user files and communications on the systems they have access to.

5. Monitoring and access in special circumstances

5.1. In special circumstances authorised University staff may access and examine the content of any data stored in, or being transmitted by, University information systems. This includes examining the content of data files and communications which should otherwise be treated as confidential and therefore goes beyond what is permitted in routine monitoring. When this takes place full details of the specific authorisation and investigation must be recorded and the records must be securely retained by the institution for an appropriate period. This will be undertaken where:

5.1.1. The Registrar considers there are reasonable grounds to suspect a specific breach of University regulations or the terms of an employment contract which justify access. (Departments wishing to access the confidential data belonging to a member of the University should make their request to the Registrar via Information Assurance Services.) This examination of data, in exceptional circumstances, may be undertaken whether or not consent is given. However; normally consent should first be requested, except where this is inappropriate because of circumstances or inadvisable because of the nature of the suspected breach.

5.1.2. The Registrar has agreed to respond to a request from a non-institutional body for information which may otherwise be subject of a court order.

5.1.3. The University is required by virtue of a Court Order or other competent authority to provide information in relation to taxation, detection and prevention of a specified crime or national security. The Registrar must be made aware of any such orders.

5.1.4. Access to a personal computer account belonging to an absent member of the University is necessary, however:

- It should not be done if it can reasonably be avoided.
- It should be done only for University business purposes and limited in scope to achieving only the purpose specified in advance.
- If appropriate, the account holder must be contacted and consent sought for access to the specific information required. Wherever possible consent should be sought and obtained in writing (email will suffice) and a record kept of the correspondence.
- Where consent is not or cannot be obtained, then written permission to access the account must be sought from the University Data Protection Officer who will specify the procedure to follow. Should the University Data Protection Officer not be available then the Registrar must be contacted.
- The Data Protection Officer or, where involved, the Registrar may require that someone supervise access to the account of the absent person.
- Accounts to which temporary access has been granted by a password change should be locked as soon as access is no longer needed.
Failure to comply with University Policy may lead to disciplinary action.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.