ICT Privacy and Monitoring Policy

1. PURPOSE

1.1 The ICT Privacy and Monitoring Policy informs the University's staff, students, and other individuals entitled to use University facilities of how, and under what circumstances, monitoring of activity or inspection of the content of electronic data assets may be carried out.

1.2 Routine activity logging of the use of ICT based systems takes place to ensure the proper functioning of those systems and to guard against unauthorized activities, and this Policy formally authorises the Director, IT and Communications Services (IT Department) to inspect these logs within defined parameters.

1.3 The Policy also identifies the exceptional circumstances when a duly authorised officer of the University is permitted to monitor, without prior consent, an individual's activity (via examination of activity logs or examination of the contents of an individual's data assets, such as e-mails or personal document files).

2. DEFINITIONS

2.1 **Activity logs:** are a by-product of many IT based systems. In general, activity logs record that a user undertook an activity rather than the content of the activity e.g. that an e-mail was sent from A to B, but not what the content of the e-mail was.

2.2 **Content Inspection:** refers to the act of examining the content of an activity e.g. looking at the body of an e-mail message. Content inspection may be targeted or broad sweep.

2.3 **Monitoring:** refers to the process of examining activity logs and/or performing content inspection for a specific purpose.

2.4 **Targeted:** content inspection refers to the process of focussing monitoring activities on an individual user or defined group of users.

2.5 **Broad Sweep:** content inspection – i.e. not targeted at individuals is generally performed by automated processes designed to ensure the proper functioning and use of IT based systems. SPAM and virus filtering are examples of broad sweep content inspection.

3. THE ICT PRIVACY AND MONITORING POLICY

3.1 The University requires that staff, students and others making use of the University's ICT-based systems are aware that activity logging takes place, and that monitoring or content inspection of an individual's activity may occur under specific circumstances.

3.2 Activity logs will be properly secured and be compliant with the University's records management policy.

3.3 The Director of the IT Department or appointed deputy is authorised to institute automated broad sweep monitoring and content inspection processes in order to ensure the proper functioning of IT systems, to validate adherence to University policy, and to guard against unauthorised activities.

3.4 The Director of the IT Department or appointed deputy may authorise targeted monitoring and content inspection only under one or more of the following circumstances:

3.4.1 To establish specific facts, as part of a formal investigation, where a Senior Manager has reasonable grounds to suspect breach of University policy or to comply with the lawful request of a third party (e.g. the police or other government agency).

3.4.2 To enable access to information crucial to the running of the University, in the absence of the individual.

3.4.3 To ensure the effective operation of a service i.e. to understand why a system appears to be performing outside its normal operational tolerances.

3.5 Where targeted monitoring or content inspection is authorised, it must be carried out in accordance with the ICT Privacy and Monitoring Procedure (Appendix A) and in accordance with the principle of minimal access to information (i.e. information so derived will be strictly controlled and only be made available to authorised recipients for specified purposes).

3.6 Those members of University staff who have the capability to access activity logs or the electronics assets of others (e.g. systems administrators) must only exercise those abilities in the context of this policy.

3.7 Individuals in breach of this policy will be subject to the Staff/Student disciplinary procedures at the instigation of the staff member with responsibility for the person concerned, in addition to potential prosecution under the Regulation of Investigatory Powers Act 2000.

4. Ownership

4.1 The Director, IT and Communications Services (IT Department) has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

A. APPENDIX A: ICT PRIVACY AND MONITORING PROCEDURE

A.1 There are three reasons to request monitoring or content inspection of an individual's use of an IT system. They are:

A.1.1 To Investigate a suspected breach of University policy or the law.
A.1.2 To access information crucial to the running of the University.
A.1.3 To ascertain why an IT system appears to be performing outside normal tolerances.

In the case of A.1.1 above, it may not always be appropriate or possible to inform the person(s) concerned.

In the case of A.1.2 above, the person(s) concerned will be approached whenever possible prior to any third party access and will be informed as soon as possible afterwards.

In the case of A.1.3 above, the Director of the IT Department or appointed deputy* will establish basic facts and remedy, with audit trail, without recourse to this procedure unless in so doing it becomes necessary under A.1.1 above.

A.2 Under A.1.1 and A.1.2, for staff a line manager must complete an online "ICT Privacy and Monitoring Form" (http://url.tees.ac.uk/forms) which will be routed to the Director of Human Resources for authorisation. If, in making the request, there is a conflict of interest (those involved in authorising or executing the request are the subject), the request should be sent, on paper, to a member of the University Executive Team (UET) for authorisation. Under normal circumstances a copy of the authorised form will be routed to the Director of the IT Department for action.

Where the subject of the request is a student, the form will be routed to the Director of Student Services for authorisation and in turn routed to the Director of the IT Department for action.

A.3 For A.1.2 where a member of staff is absent, the line manager, with permission of the relevant Dean/Director, should seek permission to access the staff member's electronic assets, through direct dialogue with the member of staff. Contact should be made in accordance with the process for contacting staff at home. The permission, or reasons for the lack of it, must be noted on the "ICT Privacy and Monitoring Form".

A.4 The Director of the IT Department or appointed deputy* will arrange the approved access and maintain an audit trail of actions taken.

A.5 The Director of the IT Department or appointed deputy* will be responsible for ensuring that any temporary access is revoked at the end of the specified period.

* The IT Department does not manage all IT based systems within the University but will act as the prime IT contact, liaising as required, in any use of this procedure. If a person from the IT Department is the subject of a monitoring or access request, Human Resources will resolve any conflict of interest.