Ulster University Standard Cover Sheet

Document Title	IT Monitoring Policy 1.7
Custodian	Deputy Director of Finance and Information Services (Information Services)
Approving Committee	Information Services Directorate (ISD)
Policy approved date	2017 – 11 – 02
Policy effective from date	2017 – 11 – 02
Policy review date	2018 – 11 – 02

Changes to previous version

UNIVERSITY OF ULSTER

Information Technology Monitoring Policy

INTRODUCTION AND BACKGROUND

The University furnishes information and communications equipment, networks, systems and services (Information Technology (IT)) to staff, associates, visitors and students with the express purpose of furthering the University's corporate aims and objectives. The University is committed to:

- Protecting its employees, students, associates, partners, itself and its investment from consequences of illegal and/or damaging use of such equipment and services;
- Ensuring the use of such equipment and services is compatible with and appropriate to its corporate aims and objectives;
- Actively managing its IT infrastructure to assure:
    - its efficient and effective operation;
    - its confidentiality, integrity and availability;
    - its capacity and performance is fit for purpose;
    - its legal operation.

The University operates its Information and communications equipment, networks and systems (including Telephony) as private systems for the use of its staff, associates, visitors and students. The University has the right, responsibility, and the necessity, to control the operation and use of its IT Systems and will therefore actively conduct monitoring of its Information Technology.

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations');
- The Counter Terrorism and Security Act (2015);

OTHER RELEVANT POLICIES, GUIDELINES AND CONTRIBUTIONS

- JISC Legal Information: E-Security Overview – Interception and Monitoring of Communications in FE and HE (2006)

AIMS, PURPOSE AND SCOPE

This policy aims to establish the University's commitment to, responsibilities for, and management framework for the monitoring of its Information Technology (IT) holdings.

The purpose is to achieve:

- Authorisation for members of staff to conduct monitoring of the University's IT;
- Effective governance and management of the use of the University's IT;
- Effective procedures for the handling of exceptions that are observed during monitoring;
- Communication of the University's responsibilities for and approach to monitoring of its IT;
- Prevention, detection and investigation of un-acceptable use of the University's IT;
- Centralised reporting and collation of incidents and co-ordination of incident management.

The scope of this policy includes all University Information Technology, Communications Equipment (including Telephony equipment), Information Systems and Services. Information Technology is potentially owned and operated by all organisation units (Faculties, Schools, Research Institutes, and Administrative Departments) within the University. The responsibility for ensuring monitoring and reporting for a given IT System lies with the Senior Officer responsible for the department managing the system;

DEFINITIONS

Information Technology Monitoring: The general, operational, management and review of IT Systems usage, behaviour and configuration; recording/logging and review of system and user actions, inspecting and auditing of the data stored, the interception of communications between IT Systems, the investigation and diagnosis of faults or incidents;

Directed investigation: The focussed collection of monitoring data, system and user data or files and/or the interception of specific communications, to investigate and collect evidence in respect of a suspected or alleged IT policy non-compliance.

PROCEDURE

Ultimate responsibility for the execution of this policy rests with the Vice-Chancellor of the University. The Information Services Directorate (ISD) is responsible for the creation and approval of this Policy's Implementation Framework and for oversight of its implementation and performance.

The Vice-Chancellor authorises Senior officers of the University and their delegates to conduct IT Monitoring.

This policy will be reviewed annually and updated as necessary to ensure that it remains appropriate in the light of relevant changes to the law, other University policies, or contractual obligations.

IMPLEMENTATION

The Policy will be implemented and supported by the introduction of codes of practice, operational and technical Standards, Procedures, and Guidelines; the Policy Implementation Framework.

Specialist advice and where appropriate, training courses or materials relating to monitoring of IT Systems shall be made available to University staff authorised to conduct activities in accordance with this policy.

The implementation of this policy shall be reviewed independently of those charged with its implementation.

It is University policy that:

1. Telephone calls may be intercepted or recorded. Telephone traffic may also be monitored by recording any of the following: date, time, duration, source, destination, and cost;
2. Requests for monitoring data from external parties, such as the police or other law enforcement agencies must be submitted in writing for approval to the Deputy Director of Finance and Information Services (Information Services);
3. All monitoring data shall be maintained in compliance with the Data Protection Act;
4. All University Information Technology shall be actively monitored. Risk assessments may be conducted and IT Monitoring activities directed and prioritised appropriately.

5. Directed investigation shall only be conducted on the written authority of the Deputy Director of Finance and Information Services (Information Services). The duration and focus of the investigation shall be limited.

This Standard shall be reviewed annually.

COMPLIANCE

Compliance with this Policy and its relevant Codes of Practice, Standards and Procedures, will be supported by:

- Implementation of appropriate information technologies for the interception, collection and inspection of computer and network data, and computer systems logs and application audit trails;
- Audit of Systems Management and administration activities on University IT Systems to ensure compliance with this and other University Policies;

The results will be subject to scrutiny by the ISD, who will in turn report their findings to senior management.

Any breaches of policy, or deliberate non-compliance with standards and procedures, will be investigated, reported and may lead to disciplinary action. The appropriate disciplinary action will be determined according to circumstance, in conjunction with the HR Department in the case of staff, and in conjunction with the relevant Dean of Faculty in the case of students. ISD will oversee disciplinary actions and report same to senior management.

In the event that an employee or student is aware of a potential breach of this policy, they are encouraged to report their concerns to their manager or Dean. All such information will be treated in confidence.

Where external organisations or individuals are using, or providing service for, the University's IT, they are required to comply with this policy, and the security standards and procedures that underpin it.

OTHER RELEVANT POLICIES

- University of Ulster Data Protection Policy
- University of Ulster Electronic Information Assurance and ISMS Policy