1. Introduction

1.1. This information security policy document contains high-level descriptions of personnel processes that must be implemented to ensure that employees are both able and required to protect the University’s information security. It is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:
   - Recruitment, references and screening
   - Employment contract terms
   - Information security education and training
   - Staff termination, suspension or change of employing department
   - IT usage monitoring and access
   - Disciplinary process
   - External parties

2. Recruitment, references and screening

2.1. For roles involving handling of confidential information or access to sensitive information systems, Human Resources may use a pre-employment screening process to help ensure that staff selected are suited to the demands of the job.

3. Employment contract terms

3.1. Staff are to sign a formal undertaking that includes:
   - Awareness that in cases of University policy violation deemed to be serious, wilful or repeated the University may take disciplinary action.
   - A confidentiality or non-disclosure agreement to protect University information both during and after their employment with the University.
   - Agreement to comply with the University Information Security policies.
   - Agreement to undertake mandatory training courses in information compliance and security as and when required by the University.
   - Understanding that, except in special circumstances, those staff granted University email addresses will be contactable via those addresses. (The University requires and so assumes that staff will regularly monitor email sent to their central service email address ensuring receipt of communications relating to University business.)

4. Information security education and training
4.1. The University is committed to providing staff with sufficient training to ensure that they are able to perform their specific information security responsibilities. Training requirements to support information security are to be reviewed during the staff appraisal process.

4.2. Information system users are to be provided with sufficient instruction or training to ensure they do not compromise security through lack of awareness or skill.

5. **Staff termination, suspension or change of employing department**

5.1. Upon termination, suspension or change of employing department, Human Resources will update the staff records system accordingly. (This is intended to trigger appropriate account management processes on centrally managed IT systems.)

5.2. Upon termination, all employees, contractors and third parties must return all information assets and equipment held which belongs to the University.

6. **IT usage monitoring and access**

6.1. The Director of Human Resources may request that legally compliant monitoring of staff e-mail be undertaken for legitimate University purposes. Policy and procedure relating to how the University may monitor usage of its IT systems (including University Mobile Phones) and the circumstances in which it may access user information on its systems and networks that is normally private is given in:

   - Institutional IT Usage Monitoring and Access (ISP-I6)

6.2. Staff will be informed upon appointment of the circumstances in which the University may access user information or monitor usage.

6.3. In line with good practice as set out by the Information Commissioner, staff will be reminded on an annual basis of the circumstances in which the University may access user information or monitor usage.

7. **Disciplinary process**

7.1. Employees who, after an investigation, have been found to have breached security or violated policy in a serious, wilful or repeated way, may be subject to disciplinary action.

7.2. Unless the police are involved from the outset, when different procedures may apply, IT Services will coordinate investigation of any suspected improper use of University IT facilities. Human Resources will coordinate any resultant disciplinary action.

7.3. Where there are reasonable grounds for suspecting misuse of a computer account, that account may be suspended by the system manager, in consultation with Human Resources, pending further investigation.

8. **External parties**

8.1. Precautions, in the form of formal agreements, should be taken to protect the information security interests of the University where external organisations or individuals are:

   - Employed to work on University information systems.
   - Provided with or given access to confidential information.

8.2. The necessary precautions relating to external parties are described in:

   - Outsourcing and Third Party Access Policy (ISP-S4)
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.