Information Security Policy

1 Scope and Purpose

Information is an asset and, as such has value which needs to be protected.
Information security is about protecting all these assets, irrespective of the media on which they are held. This is necessary in order to ensure business continuity, to meet legal, statutory and contractual obligations, and is good practice.
This Policy forms part of the University's **Information Framework**. It also underpins other University policies, such as the **Data Protection Policy** and **Quality Assurance in Research**, which seek to assure the quality of University activities and their compliance with relevant legislation.
The scope of information covered by this Policy is wide and covers all University records. All information recorded within the scope of University activity may be considered a University record, whether it is a RISIS record, a promotional leaflet or an email message about lunch. Staff have a duty to ensure appropriate keeping and/or disposal of all information they create and handle.
This Policy, together with the **Records Management Policy** and the **Guidelines for record retention and disposal** , specifies minimum requirements and procedures, and practical implementation guidelines for those creating, holding and using University information. The policy guidelines are supported by appropriate advisory/support services, training, publicity and documentation regarding risk assessment processes and consequent security measures.

2 Standards

The Policy draws on the **UCISA Information Security Toolkit** which seeks to protect the University information assets from three key risks:

Confidentiality	- inappropriate access
Integrity	- inappropriate change or destruction
Availability	- inappropriate (loss of) accessibility

3 Governance and Responsibilities

The Policy has been approved and endorsed by the University Executive Board (UEB) and University Council.
Responsibility for information security rests with every provider and holder of University information. The policy guidelines indicate the detail of such responsibilities. In addition, some general responsibilities are:

- UEB, on behalf of the University Council, is to promote the Policy and associated guidelines and monitor implementation throughout schools and services to ensure adequate security for the University's information resources.

- Members of UEB have the responsibility to seek advice regarding security matters, including any inadequacy of implementation, and resource and support requirements, and to escalate any problems that threaten security of the University's information to the Vice-Chancellor.
- Heads of Service have custodial responsibility for key information sets and information management and storage services, as detailed in the relevant guidelines.
- Heads have responsibility to ensure implementation within their school or service.
- All individuals (ie staff, students and others, including staff in organisations associated with the University) have a responsibility to adhere to the relevant policy guidelines, when creating, handling or storing University information.

Internal and external auditors will provide additional monitoring with both routine and ad hoc audits, as deemed appropriate.

Version	Keeper	Reviewed	Approved by	Approval date
1.0	ITS	Four year cycle	ISC	01/10/06
1.1	IMPS	Bi-annually	ISPC	04/09/12
1.1.1			IMPS review	30/05/14
1.1.2			IMPS review	15/09/15