

Information Security Policy (2008)

1 Aims

- 1.1 Information is vital to the operation and administration of the University, and the security of this information, and the assets associated with it, are fundamental to its continuing success.
- 1.2 There are three key aspects to information security:
 - 1.2.1 Confidentiality: information is available only to those authorised to have access
 - 1.2.2 Integrity: information is reliable, as it is accurate and complete
 - 1.2.3 Availability: information is accessible whenever and wherever required
- 1.3 The aim of this policy is to summarize and bring together the current sources of policy, regulations, procedures and guidelines, relating to information security. The intention is to make it easier for members of the University to understand their obligations.

2 Principles

The following are the guiding principles for Information Security:

- 2.1 The University will comply with relevant legislation related to information security.
- 2.2 The University's approach is based on published best practice and guidance from the Joint Information Services Committee (JISC) and standards such as ISO27001, although it is not intended to seek formal certification to any standard at this time.
- 2.3 All members of the University are responsible for information security and must conform to all University policies and procedures, and to take into account the agreed guidelines.
- 2.4 The University seeks to build a culture of information security awareness by members of the University.
- 2.5 The University will constantly seek to review and improve information security.
- 2.6 The approach will be to implement information security by policy and education rather than technology enforcement, and only where necessary impose solutions or systems to enforce best practice.
- 2.7 Information security should not hinder the legitimate work of the University.
- 2.8 User rights and access to information will at all times be based on a person's role and need rather than their status.
- 2.9 Information will only be used for legitimate academic and administrative purposes.

3 Supporting Documents

This policy gives the high level statement of Information Security strategy at the University. To support this, there will be the following documents:

Regulations for Acceptable Use of University Information Technology	The formal regulations governing computer use, and local acceptable use policy. Includes a statement on user access to systems and how that will be managed, and responsibilities of users. Also linked is the JANET AUP with which all members must also comply.
Information Security Procedures	This is a more detailed set of guidelines, covering all aspects of Information Security, based on JISC guidance and ISO27001.
You and Computers at Work	A simple, readable and understandable summary of all these policies and regulations.
Data Protection	Policy on Data Protection.
Email Usage Policies	Staff and student policies on email use.
Internet Access Policy	Policy on user access to the Internet, and any monitoring and blocking of sites
IT Disaster Recovery and Business Continuity Policy	Policy governing what will be done to recover from any significant incident, as well as policy on how system owners and users should plan to continue to deliver business function when systems are unavailable.
IT Investigation Policy	Formalising the process under which authorised staff will investigate suspected or reported breaches of security.

Document control/change history

Version	Author(s)	Date	Circulation	Comments
1	IE	23 Feb 2008	IS policy group	First draft, based on document seen by ISC
2	IE	1 May 2008		Redraft
3	IE/RM	Sept 08		Final edit and tidy

Document approval and review

Approved by:	Information Systems Committee
Date approved:	
Review date:	
Author(s):	Head of Computing Services
Owning Department:	Computing Services