

IT Services

INFORMATION SECURITY POLICY

OVERVIEW AND PURPOSE

- 1.1. information technology services underpin all of
 - through teaching and research to the benefit of the wider community.
- 1.2. The University recognises the need for its staff, students, associates and visitors to have access to the information and/or information technology services they require in order to carry out their work and study and recognises the role of information security in enabling this.
- 1.3. The University also recognises the information it manages must be appropriately secured in order to protect the institution and its stakeholders from consequences of breaches of confidentiality, failures of integrity or interruption to availability of information, and to maintain its reputation for trustworthiness.
- 1.4. order to maintain business continuity, legal compliance and adherence regulations and policies, including the Regulations for the Use of Information Technology.
- 1.5 The University is committed to maintaining a safe, welcoming and inclusive environment.

 Encouraging debate and discussion, and upholding freedom of speech is to be balanced with our legal obligations. The Counter-Terrorism and Security Act 2015 places an obligation on

er details can be

found on our website.

- 1.5. Objectives
 - 1.5.1. To define the framework within which information security will be managed across the University.
 - 1.5.2. To demonstrate management direction and support for information security throughout the University.

1.5.3. security a

- 1.6. Principles
 - 1.6.1. Security controls must be put in place to ensure that confidentiality, integrity and availability of information is assured. Controls should be commensurate with risk but must always adhere to minimum standards set by University policies and legal/regulatory standards. Security controls must be maintained when information is taken off-site, accessed from off-site or accessed using mobile technologies.
 - 1.6.2. Information must be processed in accordance with the Data Protection Policy and the Records Management Policy. Consideration should be given to classifications assigned to

Document Control Document Control					
Document No	ISP01	Version	5.0	Date Issued	20 Oct 2020
Author	Pete Collier	Reviewed by	IGC	Department	ITS

information (see Information Classification and Handling Policy) and the consequent access granted to staff, students and associates of the University and third parties.

- 1.6.3. Transfers of information to third parties must be made adhering to relevant policies and must be authorised at an appropriate level. A data sharing agreement must be in place unless the data transfer is defined and constrained in a contract. Minimum agreed levels of security controls must be maintained. Transfer to third parties includes use of cloud or third party hosted services by individual users.
- 1.6.4. The University shall ensure its information technology services and third-party arrangements are designed and configured with sufficient and appropriate measures implemented to minimise the risk of information security breaches.
- 1.6.5. All incidents involving actual or potential breaches of information security must be reported and managed in accordance with the Information Security Incident Reporting Process. The University will investigate all security incidents and take appropriate action in accordance with this policy, University Regulations, and English Law.
- 1.6.6. All information security measures, and policies defining them, will be regularly reviewed and tested, including use of annual internal audits and penetration testing.

2. SCOPE

- 2.1. This policy applies to all use of University information technology services including software, computers and/or networks, whether on-campus, via remote connections or in doud services.
- 2.2. Use of devices not owned or supplied by the University is also covered if connecting in any way to University provided information technology services.
- 2.3. This policy applies to all users of University provided information technology services

Document Control					
Document No	ISP01	Version	5.0	Date Issued	20 Oct 2020
Author	Pete Collier	Reviewed by	IGC	Department	ITS

The Director of IT Services is responsible for overall technology security measures protecting the University, including proactive defence, monitoring and incident response.

- 3.4.1. Proposing required changes to the Information Security and subsidiary policies to the Information Governance Committee for approval.
- 3.4.2. Overall implementation management of the Information Security and subsidiary policies.
- 3.4.3. Ensuring information technology services used by

Document Control					
Document No	ISP01	Version	5.0	Date Issued	20 Oct 2020
Author	Pete Collier	Reviewed by	IGC	Department	ITS