IT Services

Document Control

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

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