GISP21. Liability of own systems and content brought to University

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	Controls to ensure that personally-owned devices connecting to the University network do not compromise security, or introduce liabilities for the University.
Objective	To ensure that personally-owned devices connected to the University network do not compromise security or give rise to any claims against the University.
Policy	21.1. All connections to the wireless network must be authenticated using valid credentials. See GISP7. 21.2. All personally owned equipment connecting to the wired network (including residences) must be registered before connection is permitted. See GISP7. 21.3. The University accepts no responsibility for either the safety or security of personally owned systems.
Responsibility	• ITCS is responsible for providing a secure network and method of connection for personally owned equipment. • Users are responsible for ensuring their personal computer systems are safe, secure and operated within legal frameworks.
Incident Management	Incidents should be reported to the IT Service Desk. If a personally owned system, or data stored on University filestore is found to be in contravention of this policy, access to the network, or data may be denied, depending on the level of risk to the University. Further action will be taken where appropriate.