201P82 0 T

- Human Rights Act 1998
- Data Protection Act 2018
- General Data Protection Regulation
- Regulation of Investigatory Powers Act 2000
- Counter Terrorism and Security Act 2015
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and 2013
- Rehabilitation of Offenders Act 1974
- Environmental Information Regulations 2004

## 3. Purpose of university information security policy documentation

3.1. University policy documentation should perform the following functions:
- Present a comprehensive and coherent approach to information technology and security at a strategic level
- Reflect the intentions of the university by defining expected standards
- Facilitate on-going development, scrutiny and revision of policies at strategic and tactical levels

3.2. Provide guidance or direction to users, administrators and developers of university information systems

## 4. Scope

4.1. This policy and associated polices detailed in Section 9 of this document apply to all information systems:
- Owned by the university
- Being used for university business
- Connected to networks managed by the university

4.2. The policies in this documentation set apply to all information:
- The university is handling whether or not it is owned by the university
- Including software owned or licensed by the university
- Managed by 3rd party processors on behalf of the university

4.3. The policies in this documentation set apply to all people:

- x Managing or using any system identified in section 4.1 above
- x Responsible to the university and handling information identified in section 4.2 above

## 5. Structure of the policy documentation s et

5.1. The structure and content of this policy documentation set is based on an approach set out in the "*University and Colleges Information Systems Association* (*UCISA) Information Security Toolkit*". The Toolkit is intended to help academic institutions to formulate and maintain policy documents, and is based on the control guidelines in the industry framework ISO27001 (2)10.5 al

- Ensuring that all individuals who use information systems, or otherwise handle information, understand the policies that are relevant to them and any consequences for non-compliance.
- Using physical security measures when deemed necessary.
- Applying technology where considered appropriate and feasible. For example, to control and log access to systems, data and functionality.
- Using various lawful forms of monitoring activities, data and network traffic to detect policy infringements.
- Taking into account relevant information security policy requirements when planning and undertaking activities involving information technology based systems.
- Formal or informal risk assessment, to identify the probability and impact that various hazards could have on information systems.
- Monitoring effectiveness of its information security policy implementation. This may involve independent review from those charged with its implementation.

## 8. Responsibilities for implementing information technology and security policies

8.1. The Chief Operating Officer is accountable for information technology and security policies at the university.

8.2. The Director of ITMS or their nominated deputy is responsible for the implementation of information technology and security policies at the university.

8.3. The Data Protection Officer or their nominated deputy is responsible for providing oversight and guidance on the compliance with the data protection regulations and on protecting individuals rights

Approved date: October 2018
Review date: September 2019
Reviewer: Interim IT Governance Manager

## 11. Document History

11.1. October 5th 2012 – Version 1 Neil Faver
11.2. September 2014 – Version 1.4 Neil Faver
11.3. January 2016 – Version 1.6 Neil Faver
11.4. 11.4 September 2018 Neil Faver