Principal Information Security Policy

1. Introduction

1.1. This policy sets out De Montfort University's definition of, commitment to and requirements for Information technology and security. It specifies regulations to be implemented to secure information and technology that the university manages and to protect against the consequences of breaches of confidentiality, failures of integrity and interruption to availability of university networks and services. It will refer to more specific policy documents covering these specific needs.

1.2. This policy provides management direction and support for information technology and security across the university. It has been ratified by the Executive Board (EB) of the university and forms part of its policies and procedures. It is applicable to, and will be communicated to, staff, students and other relevant parties. This document includes:

- Legal requirements that the university must abide by
- The purpose, scope and structure of the information technology and security policy documentation
- Responsibility for information technology and security policy documentation
- Implementing information technology and security policies
- Responsibilities for implementing information technology and security policies
- References to related documents.

1.3. This policy provides the overall structure for information security, including a number of sub-policies that define the approach of the university. This policy outlines the scope and responsibility of the university board and committees, the key responsible officers and the overarching approach and strategy. The sub-policies provide further information on the responsibilities of managers and staff in supporting the approach to information security.

2. Legal requirements

The university will abide by all UK legislation and relevant legislation of the European Community related to the holding and processing of information. This includes the following acts and the guidance contained in the Information Commissioner's Codes of Practice:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1999
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990

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

5. Structure of the policy documentation set

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

5.2. Specific, subsidiary information technology and security policies shall be considered part of this policy and shall have equal standing

5.3. This policy and associated policies shall be reviewed annually in the light of any relevant changes to the law, organisational changes or contractual obligations, to ensure its continuing sustainability, adequacy and effectiveness

5.4. Each strategic policy document shall contain only high-level descriptions of expectations and principles; they are deliberately free from practical details of policy implementation

5.5. Where necessary, details expanding on how statements in the strategic policy documents are to be implemented should be described as *Policy Implementation* documents

5.6. Where necessary, PVC/Deans of Faculty or Directors may request to implement different policies relating to the use of IT systems for which they have responsibility, subject to agreement with the Director of Information Technology and Media Services (ITMS)

6. Responsibility for information technology and security policy documentation

6.1. The university's Executive Board through its delegated authority (ITSG, the IT Strategy Group) has ultimate responsibility for approving updates and additions to the University information technology and security policy documentation set

6.2. The Information Governance Board is the information security oversight committee reporting to ITSG. The objective of this board is to ensure that there is clear direction and management support for information security issues

6.3. The Data Protection Officer is responsible for providing oversight and guidance on the compliance with the data protection regulations and on protecting individuals rights for this

6.4. Proposed changes and additions to the policy documentation may be submitted by any member of staff, via a Dean of Faculty or Director, to the Director of ITMS or delegated authority before consideration at the Executive Board or appropriate sub-committee

6.5. Proposed updates to policy must be fully converted into proposed changes to the policy documentation. This must be done in such a way that implications for all related documents are fully taken into account

7. Implementing information technology and security policies

7.1. Measures will be taken by the university to implement information technology and security policies including:

- Establishing a continuous *Plan-Do-Check-Act* cycle of activities which ensure that suitable practices are documented reinforced and improved with time. (Documentary evidence of the processes and procedures involved will be required to demonstrate implementation of policy to external parties).

- 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 for this
8.4. The Threat Management Group is responsible for identifying and assessing risks and threats to the security of information at the university, and for recommending the appropriate mitigations
8.5. It is the responsibility of the university to sufficiently resource and direct implementation of these policies.
8.6. Individuals must understand and agree to abide by university information technology policies and regulations before being authorised for access to any information systems for which the university has responsibility.

9. References to strategic level policy sub-policies

- Outsourcing and Third Party Access Policy
- Information Handling Policy
- Use of Computers Policy
- User Management Policy
- System Planning and Management Policy
- Network Management Policy
- Software Management Policy
- Encryption Policy
- Mobile Computing Policy
- Records Management Policy
- Records Disposal Policy
- Research Records Management Policy
- DMU Data Protection Policy

10. Document Approval

Approved by: Chair of the Information Governance Board

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