Information Handling Policy

1. Introduction

1.1. This policy sets out De Montfort University's definition of, commitment to and requirements for Information Handling. It sets out the need to define classes of information handled by the organisation and the requirements for the storage, transmission, processing and disposal of each. Requirements may include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups). This policy should be familiar to all staff dealing with information.

1.2. This information handling policy provides management direction and support for information handling across the university. This policy has been ratified by the Executive Board 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:

1.2.1. The purpose, scope, definitions of the Information Handling policy.
1.2.2. Responsibility for information Handling Policy documentation.
1.2.3. Responsibilities for implementing information handling policies.
1.2.4. References to related documents.

2. Purpose of University Information Handling Policy Documentation

University policy documentation should perform these functions:

2.1. Present a comprehensive and coherent approach to information security at a strategic level.
2.2. Reflect the intentions of the University by defining expected standards.
2.3. Facilitate on-going development, scrutiny and revision of policies at strategic and tactical levels.
2.4. Provide guidance or direction to users, administrators and developers of University information systems.

3. Scope

The policies in this documentation set apply to all information:

3.1. The University is handling whether or not it is owned by the University.
3.2. Including software owned or licensed by the University.

4. Classes of information

4.1. All information held should be classified according to the following definitions:

- **Unclassified information** – information which is not confidential or personal and which may be disseminated freely.

- **Personal information** – information covered by the Data Protection Act 1998 which allows a living individual to be identified or which relates to an identifiable individual.
- **Sensitive Personal information** – information covered by the Data Protection Act 1998 which relates to an individual's ethnicity, political membership or opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission of an offence and any related proceedings.
- **Confidential information** - information which may or may not be personal and which may not be disclosed except to those with the explicit consent of the data owners and where disclosure may constitute an actionable offence.

4.2. Security arrangements appropriate to the classification level must be in place at all times to ensure the integrity of the information.

4.3. The retention period of each class of information held should be determined according to the University Retention Guide. Information should not be kept longer than it is required for business use, unless required for inclusion in the University archives.

5. Inventory, Management and Ownership of Information

5.1. A full inventory will be held and maintained by each Faculty/Directorate of all important information assets.
5.2. Each asset will have a nominated owner, although responsibility for the security measures may be delegated to a nominated individual, accountability remains with the owner.
5.3. It is recommended that an annual review of information assets held by each Faculty/Directorate is performed.

6. Disposal of Information

6.1. Any paper documents with a classification of sensitive or above must be shredded.
6.2. When permanently disposing of equipment containing storage media, all data and software must be irretrievably deleted by using an in-house procedure or by another licensed organisation.

7. Information on Desks, Screens and Printers

7.1. The possibility that confidential information may be viewed on a screen by unauthorised persons must be considered when siting devices in a room or office space.
7.2. Staff responsible for handling confidential paper documents must take appropriate action to avoid unauthorised disclosure. Procedures must be in place based on the nature of the document. This may include locking the document away when not in use.
7.3. When printing or copying any confidential data, the device or printer must be physically secure or attended.

8. Exchanges of Information

8.1. Intended third party recipients of classified information or documents must not only be authorised to receive such information, but have ensured they have sufficient information security policies and procedures in place to assure the confidentiality and integrity of the information.

8.2. Personal, Sensitive or Confidential data or information, may only be transferred across networks, or copied to other media, once it has been encrypted and password protected. Transfer should only occur when the confidentiality and integrity of the data can be reasonably assured throughout the transfer.

8.3. All parties are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

8.4. Email addresses and faxes should be checked carefully prior to dispatch, especially where the information content is sensitive; and where the disclosure of email addresses or other contact information to the recipients is a possibility.

9. Implementing Information Handling Policies

Measures will be taken by the University to implement information security policies including:

9.1. 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.)
9.2. 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.
9.3. Using physical security measures when deemed necessary.
9.4. Applying technology where considered appropriate and feasible. For example, to control and log access to systems, data and functionality.
9.5. Using various lawful forms of monitoring activities, data and network traffic to detect policy infringements.
9.6. Taking into account relevant information security policy requirements when planning and undertaking activities involving IT-based information systems.
9.7. Formal or informal risk assessment, to identify the probability and impact that various hazards could have on information systems.
9.8. Monitoring effectiveness of its information security policy implementation. This may involve review independent from those charged with its implementation

10. Responsibilities for Implementing Information Handling Policies

10.1. It is the responsibility of the University to sufficiently resource and direct implementation of its information handling policies.

10.2. Individuals must understand and agree to abide by University policies before being authorised for access to information from systems for which the University has responsibility.

10.3. Where responsibility for applying the University Information Handling Policy to Faculty or Directorate information systems is delegated by the University to the Deans of Faculty or Director respectively, they are responsible for any further delegation of functions relating to policy enforcement.

11. References to Strategic Level Policy Sub-Documents

11.1. Principal Information Technology and Security Policy

11.2. Outsourcing and Third Party Access Policy
11.3. User Management Policy
11.4. Use of Computers Policy
11.5. System Planning and Management Policy
11.6. Network Management Policy
11.7. Software Management Policy
11.8. Mobile Computing Policy

12. Document Approval

Approved by: Kathryn Arnold CIO
Approved Date: 5th October 2012
Review Date: 5th October 2013
Reviewer: IT Governance Manager

13. Document History

13.1. 24th December 2010 – Draft 1 Fraser Marshall
13.2. 30th January 2011 – Draft 2 Neil Faver
13.3. 21st February 2011 – Draft 3 Neil Faver
13.4. 13th June 2011 – Draft 4 Neil Faver
13.5. 6th September 2011 – Draft 5 Neil Faver
13.6. 5th October 2012 – Version 1 Neil Faver