MANCHESTER 1824
The University of Manchester

**Standard Operating Procedure**

| | | | |
|---|---|---|---|
| **Title:** | **Information Security Responsibilities** | | |
| **Version:** | **1.2** | **Effective Date** | **June 2013** |
| **Summary:** | **Describes the governance framework and responsibilities for information security** | | |

**When using this document please ensure that the version you are using is the most up to date by checking on the University's online document system http://documents.manchester.ac.uk/list.aspx for any new versions.**

## 1 Purpose

The purpose of this procedure is to specify the responsibilities which support the implementation of the University's Information Security Policy.

## 2 Governance and responsibilities

**2.1 Board of Governors – Registrar, Secretary and Chief Operating Officer (RSCOO)**
The Board of Governors is responsible for establishing the broader University policy framework and authorise the RSCOO to issue and review policy statements and procedures to support University Ordinances and Regulations with which Members of the University must comply.

**2.2 Risk and Emergency Management Group (REMG)**
The RSCOO receives assistance from REMG in carrying out these responsibilities which, in relation to information security, includes:

- approving plans, procedures, guidance documents and support material produced to assist staff, students and other approved users in discharging their information security responsibilities
- receiving regular reports on information security Issues
- receiving reports on information security auditing and performance monitoring throughout the University
- providing regular reports to Board Committees including proposed changes to University polices and procedures

**2.3** The **Senior Executive Team** will be consulted on all matters relating to policies and procedures and are responsible for promoting adoption within their respective areas of operation.

**2.4 All Heads of School/Directorate/Office** are responsible for implementing the policy within their area and for compliance by their staff including:

- managing the risks to information security within their area and ensuring that security arrangements are proportionate to the level of risk
- the provision of appropriate physical arrangements for the secure storage of data held on paper and electronic media, in line with the University's policies, procedures and guidelines for such matters
- the provision of appropriate disposal mechanisms for paper and electronic records which are in line with University-approved arrangements, preserving confidentiality as required, and cognisant of the University's and funding bodies' records retention requirements
- where appropriate, determining access rights to information (such as information held on the University's administrative applications) in collaboration with Information Owners and establishing an appropriate regime for monitoring access to confidential and personal information, electronic or otherwise, and provide evidence of such monitoring
- ensuring that all staff are aware of their information security responsibilities and receive appropriate information security guidance and training relevant to their job role, maintaining records as evidence eg through the performance and development review process
- assigning generic and specific responsibilities for information security management

- encouraging all managers and student supervisors to lead by example

**2.5** **Information Owners** play a key role in protecting information, in that they understand the value of the data and are therefore responsible for specifying, implementing and monitoring safeguards to protect the confidentiality, integrity and availability of the information throughout its lifecycle. This includes establishing controls which manage the creation, storage, access, distribution, amendment, copying, archiving and disposal of information. If the information is held electronically this includes providing appropriate IT security, in line with the policies, procedures, guidance or advice provided by IT Services or as specified by any contractual arrangements with outside bodies (eg NHS Trusts) where these are more stringent.

Information Owners including the authors of research papers, dissertations, databases or spreadsheets must, at inception, consider the information's exposure to risk and take steps to mitigate these risks, particularly where the information contains personal or confidential information or data which would be difficult to reproduce if lost.

In more complex scenario where the information is created and accessed by many users (such as the University's administrative applications) the Information Owner of the service must be clearly stated. Whilst it may be necessary to delegate the implementation of specified controls, the Information Owner must establish an appropriate monitoring regime to obtain assurance and evidence that the controls are operating as required.

Information Owners are responsible for ensuring compliance with the provisions of data protection laws and good practice, or other legislation pertinent to the data being held, and for retaining information in line with the University's Records Retention Schedule or funding body retention requirements where these are more stringent.

Ownership in this context does not relate to ownership of the intellectual property in the data.

**2.6** **All authorised users** of information are responsible for its safe custody. Anyone who has access to information whether as a user of a software application or as a recipient of information via electronic, paper or verbal means, is required to keep the information secure to the level required by the Information Owner.

Authorised users:

- do **not** have the right to grant access to or alter the data in any way without the approval from the Information Owner.
- may **not** take copies or extracts of confidential or personal data off University premises or onto portable electronic media without the specific, documented permission of the Information Owner, and then only provided that appropriate security arrangements are in place eg encryption of electronic data.
- may **not** share confidential or personal information with anyone without the express permission of the Information Owner.

Where an authorised user takes a copy of the information, they become personally responsible for implementing the same controls to protect the information as those expected of Information Owners.

**2.7** **Project Managers and Researchers** must ensure that information security activities are built into both the delivery and resource plans of their projects. Where personal or sensitive information is likely to be obtained, advice in relation to the requirements of data protection laws and good practices must be sought from the Records Management Office. Where research is undertaken by students, the responsibility for appropriate data handling lies with the supervisory staff.

**2.8** **The Director of IT** is responsible for providing expertise in relation to IT security including:

- developing, implementing and communicating IT security policies, defining technical information security standards and security architectures

- working with Information Owners to assess risks, identify IT controls proportionate to the risk/impact which are in line with business requirements
- undertaking security reviews and investigations relating to IT issues
- providing secure disposal of confidential data held on electronic media

Where the information is held within approved University applications or systems, IT Services are responsible for:

- the safe custody of the data and its availability and provision to those authorised to use it
- implementing controls and monitoring the effectiveness of controls in line with business requirements
- the integrity of the systems, applications and integration between applications, and the code that manipulates data
- controlling the access routes to such systems and applications including the use of portable devices and access from remote locations

**2.9** **The University Librarian** is responsible for acquiring and providing access to scholarly information resources (licensed content, University research and teaching outputs and digitized materials) and their archiving and preservation.

**2.10** **The Director of Communications and Marketing** is responsible for corporate information on the University website.

**2.11** **The Director of Estates and Facilities** is responsible for the provision of advice and guidance on the security of premises and approved arrangements for the secure disposal of confidential papers.

**2.12** **The Deputy Secretary** has responsibility for general information policies and associated legislative compliance and, through the **Records Management Office**:

- provides advice and guidance to staff on their legal obligations under the Data Protection Act
- provides records retention and disposal advice in line with the University's Records Retention Schedule
- co-ordinates responses to subject access requests made under the Data Protection Act and information requested under the Freedom of Information Act or the Environmental Information Regulations

**2.13** **The Information Security Manager** has responsibility for:

- monitoring compliance with this and the associated policies and procedures which describe the measures taken by the University to protect its information
- ensuring that expert advice, guidance and training on the implementation of such policies is available
- ensuring that risks to information security are appropriately managed

## 3 Monitoring and auditing

The successful implementation of these procedures is measured by:

- Review of local risk registers
- Annual Compliance Exercise
- Feedback from staff and students
- Analysis of the responses and audits of funding organisations
- Review of the frequency of security incidents
- Risk-based programme of audits of staff and systems

**If you are reading a printed version of this document you should check**
**http://documents.manchester.ac.uk/display.aspx?DocID=8039**
**to ensure you have the most up to date version**

**Version amendment history**

| Version | Date | Reason for change |
|---|---|---|
| 1.0 | June 2010 | Creation |
| 1.1 | October 2011 | Updated links to related policies and procedures |
| 1.2 | November 2014 | Updated links and change of job titles |

| **Document control box** | |
|---|---|
| Policy / Procedure title: | Information Security Responsibilities |
| Date approved: | June 2010 |
| Approving body: | Risk and Emergency Management Group |
| Version: | 1.2 |
| Supersedes: | IT Services Information Security Policy |
| Previous review dates: | November 2014 |
| Next review date: | August 2015 |
| Related Statutes, Ordinances, General Regulations: | Statute XIII Part III re disciplinary procedures for staff;<br>Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems;<br>University General Regulation XV Use of Information Systems;<br>University General Regulation XVII Conduct and Discipline of Students – (I) re misuse of property and information systems |
| Related policies: | Information Security Policy:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525<br>Data Protection Policy:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914<br>Freedom of Information Policy:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14915<br>Records Management Policy:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14916<br>Acceptable Use Policy – IT facilities and services:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16277<br>IT Information Handling, Encryption and Mobile Computing:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=19983<br>IT User Management Policy:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=19982<br>IT Operations Policy:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=19981<br>IT continuity management and planning:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=19979 |
| Related procedures: | Acceptable Use of IT Facilities and Services - Standard Operating Procedure for Staff:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221<br>Acceptable Use of IT Facilities and Services - Standard Operating Procedure for Students:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16220 |
| Related guidance and or codes of practice: | Data Protection Guidance:<br>http://www.dataprotection.manchester.ac.uk/<br>Records Retention Schedule:<br>http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514 |

| | |
|---|---|
| | IT Security guidance:<br>http://www.itservices.manchester.ac.uk/secure-it/ |
| Related information: | |
| Equality relevance outcome: | Low |
| Policy owner: | Director of Compliance and Risk |
| Lead contact: | Information Security Manager |