MANCHESTER 1824
The University of Manchester

Standard Operating Procedure

Title:	Information Security Classification, Ownership and Secure Information Handling		
Version:	1.3	**Effective Date**	October 2016
Summary	Procedure for allocating information security classifications and appropriate information handling		

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 Background and purpose

The University handles a wide variety of information which is often shared internally and with outside organisations and individuals. The use of some information is constrained either by legislation, such as current Data Protection and Export Control legislation, or in order to protect the interests of the University, whilst other information may need to be made freely available, such as information in response to Freedom of Information legislation requests and research papers. Balancing the tension between the secure handling of information and operational efficiency requires an assessment of the risks involved and makes it difficult to provide a prescriptive procedure for the plethora of University activities and information. Consequently this Standard Operating Procedure **("Procedure")** describes generic requirements which must be considered in relation to all information handling processes.

The purpose of this Procedure is to:

- Establish information security classifications for use by the University;
- Provide guidance for Information Owners in applying information security classifications;
- Ensure that appropriate baseline controls are applied which are commensurate with the selected information security classification;
- Clarify appropriate information handling to minimise risk; and
- Minimise the University's exposure to financial loss, reputation damage or legal proceedings arising from a breach of the confidentiality, integrity or availability of information.

Caveat:

- The University is publicly accountable and is subject to Freedom of Information requests, and requests from individuals to access their personal data in accordance with current Data Protection law. Such requests will be subject to scrutiny in relation to appropriate exemptions, public interest and legal considerations, but information related to University activities may be made available regardless of any information security classification, or the media on which it is held eg non-University email accounts, non-University-owned devices or storage.

2 Definitions and scope

Information - For the purposes of this Procedure, information includes the raw data from which information is derived.

Information store – where information is held/stored, for example, paper records in a filing cabinet, data held in IT systems, records stored onsite and offsite (eg in the Cloud), approved encrypted removable media. This list is not intended to be exhaustive.

Information processing activities - eg obtaining, recording, viewing, holding, altering, disclosing / sharing, destroying information, including information processed by third-parties on the University's behalf. This list is not intended to be exhaustive.

Collectively information stores and processing activities are known as **information assets**.

Information Store Owners are accountable for information held within the information store including the approval of any processing activities. For example the Director for the Student Experience is accountable for information processed in Campus Solutions. Where the information in an information store is created through many processing activities and accessed by many users (such as the University's administrative applications) the Information Store Owner may delegate responsibility for the processing activities to a Processing Activity Owner. Information Store Owners also include, for example, the authors of research papers, dissertations, databases or spreadsheets (this list is not intended to be exhaustive) where they may also be the Processing Activity Owner.

Information lifecycle – the information lifecycle describes the stages a record or piece of information goes through, from creation through being an active record (ie one which is used on a regular basis) to a semi-active record (one which needs to be kept but which is less frequently used) to disposition (archiving, destruction).

Information Security involves consideration of the following aspects:

- **Confidentiality** – concerned with preserving authorised restrictions on information access and disclosure, including the protection of person identifying information ("PII") and proprietary information.
- **Integrity** – concerned with guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- **Availability** – concerned with ensuring timely and reliable access to and use of information.

This Procedure applies to:

- All members of staff, as well as individuals conducting work at or for the University and/or its subsidiaries, who are duly authorised to have access to University data **("staff")**. This includes temporary, honorary, visiting, casual, voluntary, agency workers, students employed by the University, and suppliers (this list is not intended to be exhaustive); and/or
- All information created or received in the course of University business which must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the location of the information, the manual or automated systems that process it, the methods by which it is distributed or the locations from which it is accessed.

3 Procedure and responsibilities

3.1 Consequence of non-compliance with this Procedure

Compliance with this Procedure is mandatory and non-compliance must be reported to the Head of Information Governance who will determine the action to be taken. Staff must note that any breach of this Procedure may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action. Serious breaches of this Procedure may constitute gross misconduct and lead to summary dismissal.

3.2 Information security classification - impact assessment

There are three aspects to consider when classifying information: confidentiality, integrity and availability. The information security classification is determined by assessing the adverse impact or damage that would occur if there was a breach in the confidentiality, integrity or availability of the information.

3.2.1 Confidentiality classification:

Information Security Classification - Confidentiality		
Highly Restricted (High Impact)	Restricted (Medium Impact)	Unrestricted (Low Impact)
Information which if disclosed to unauthorised persons would have a significant adverse impact eg: • Significant distress or financial loss to individuals[1] • Significant fines and enforcement action by the ICO for data breaches; • Significant reputational damage; • Withdrawal of one or more significant research grants or donations; • Litigation against the University; and/or • Significant financial loss due to premature disclosure of IP.	Information that, whilst not classified as Highly Restricted, could result in harm or distress to individuals[1] or the University if there were an accidental, deliberate or unlawful breach in confidentiality.	Information where a breach in confidentiality would result in little or no adverse effect on individuals[1] or the University
Examples of information in these classifications can be found in http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=15677 with the caveat that the examples are provided as a guide and not a defined list, as the circumstances of each case must be considered in order to assess the harm that might occur to any individuals concerned, or the impact on the University, should there be a breach of confidentiality.		

3.2.2 Integrity classification:

Information Security Classification - Integrity		
Critical (High Impact)	Important (Medium Impact)	Low value (Low Impact)
Information that is indispensable or essential to maintain University operations and/or to maintain integrity of University assets, and/or to protect individuals;	Information that is fundamental to maintain University operations and/or to maintain integrity of University assets, and/or to protect individuals; where the	Information that is lacking in value to maintain University operations and/or to maintain integrity of University assets, and/or to protect individuals; although susceptible to

[1] For example: students; customers; alumni; applicants; donors; potential donors; parents of current or former students; current, former and prospective employees; research volunteers; patients.

Information Security Classification - Integrity		
Critical (High Impact)	Important (Medium Impact)	Low value (Low Impact)
where loss of, or inaccuracy in, this information could result in severe operational impact and/or give rise to severe financial, regulatory or reputational consequences. *eg 99%-100% error free expected.*	consequences of inaccuracy or a loss of integrity will be less severe than is the case for critical information. *eg 95-98% error free information is expected.*	integrity breaches, inaccuracies would not result in significant business consequences. *eg less than 95% error free information.*

3.2.3 Availability classification:

Information Security Classification - Availability		
Critical (High Impact)	Important (Medium Impact)	Low value (Low Impact)
Describes information assets where availability (and the expectation of availability) is imperative to the operation of the University; any failure of availability would result in a severely impaired ability to make management decisions, impact key control procedures and may result in a legal liability, loss of public confidence and significant costs arising from workarounds and restoration of service. *eg no interruption of access beyond 4 working hours is expected.*	Information assets where routine availability is embedded in the normal operation of the University; loss of availability would result in a degraded ability to make management decisions and operate normal control procedures, but if restored within appropriate limits would be unlikely to result in legal liability, loss of public confidence, or costs arising from workarounds and restoration of service. *eg no interruption of access beyond 8 service hours is expected*	Information assets where loss of availability would result in a degraded ability to undertake some aspect of University operations but is unlikely to impact upon the ability to make management decisions, operate control procedures and, whilst inconvenient, would not lead to legal liability and is unlikely to result in a loss of public confidence; the costs arising from workaround/restoration are likely to be low, but proportional to the asset nature. *eg interruption of access may extend beyond 24 hours or be in the next planned release for approval.*

3.2.4 Other factors affecting impact:

The impact level, and therefore its security classification, may be affected by a number of factors such as:

- Timing – For example, information that was once considered to be Restricted may become Unrestricted once it has been appropriately discussed and approved eg University financial forecasts and budgets, research papers prior to publication; the availability of specific systems may be more critical at certain times of year eg admissions systems during clearing;
- Volume of data - For example, the personal data of one individual which would normally be classified as Restricted, may be Highly Restricted where thousands of records are involved; errors are more difficult to spot in high volumes, so methods to protect the integrity of information are more critical; manual processes may not be feasible if systems which process high volumes become unavailable, so availability is more critical;
- Context – For example, personal data belonging to someone whose physical safety is at risk may be categorised as Highly Restricted rather than Restricted;
- Legal or contractual requirements – the most restrictive security classification must apply where information is subject to specific protection requirements under a contract, grant, local procedure or export control regulations.

If a package of data elements contains differing classifications of data, the Information Asset Owner must assign the entire package the highest information security classification included within the package. For example, if a report contains both “Restricted” and “Unrestricted” information, the complete report must be classified as “Restricted”.

3.3 Secure information handling – minimising the likelihood of an incident

The likelihood of information being jeopardised depends on the processes which affect it eg where it is stored and accessed, how it is shared, how it is disposed of. A layered approach, involving physical and technical controls which create obstacles to deter unauthorised access, helps to minimise the likelihood of an information security incident. Controls must be selected which are appropriate to the information security classification but must also be balanced with ease of access required by authorised users. The mandatory minimum protection and security controls for each classification can be found in the Information Handling Minimum Controls (see Appendix A).

In exceptional cases, the likelihood of a **targeted** attempt to access information may increase, for example, if the subject matter is:

- Politically sensitive eg research to prove or undermine a government’s political stance;
- News-worthy eg provides the basis of an article deemed to be in the public interest;
- Financially beneficial eg valuable research, intellectual property or high volumes of personal data which could be sold to external organisations;
- Research data known to be at particular risk of being targeted by foreign states

Other examples can be found here. In such circumstances additional precautions may be required and advice must be sought from the University’s Head of Information Governance.

3.3.1 Storage and access controls

- All information must be stored and handled in a manner appropriate to its security classification, and the master copy of all digitally held information, regardless of its security classification, must be stored on University-approved systems.
- Temporary storage of Highly Restricted or Restricted information outside of the University-approved systems require the file, device or media to be encrypted and the device or media to be kept physically secure at all times.
- Highly Restricted or Restricted information on live systems must not be used for testing or training (eg copied to test environments or used in screen shots).
- Highly Restricted information must always be encrypted, including data on University systems and with third-party/cloud service providers.

3.3.2 Protective marking

Protective marking is often used to make it clear to the reader that the information has restricted circulation and requires additional safeguards to protect it. It usually involves displaying the confidentiality marking (eg Restricted, Highly Restricted) somewhere on each page of a document or in the filename.

It is not the intention of this SOP to mandate that all information is protectively marked, though this is best practice and is encouraged to align with the strategic direction for information security.

3.3.3 Sharing Restricted or Highly Restricted information - principles

Whenever information is shared, the exposure to risk increases. Contact IT Services for advice on selecting the most appropriate collaboration tool.

Restricted and Highly Restricted information must only be shared in accordance with the following principles:

- There must be an acceptable reason why the recipient needs the information;
- Only the minimum, essential information and nothing more must be provided. Wherever possible the information must be desensitised by removing non-essential Highly Restricted information;
- The person sharing the information must have permission to share it. This may involve consulting with the Information Asset Owner or others prior to disclosing the information;
- Restricted or Highly Restricted person identifying information must never be shared with external organisations or people, including the police and legal advisers, without first consulting the Information Governance Office;
- Export controlled information must only be shared in accordance with the relevant University procedure – such information will normally be classified as Highly Restricted;
- Contracts with third-parties who may be collecting or processing personal data on the University's behalf must comply with the University's requirements in relation to privacy and security, and both the Information Governance Office and relevant IT Relationship Manager must be consulted before engaging such services. See "Acquisition, development and maintenance of IT systems, and/or services" Standard Operating Procedure for further information.

3.3.4 End of lifecycle

- Information must be kept in accordance with the University's Retention Schedule which specifies a minimum retention period for master copies of records. Local arrangements or contractual requirements may specify a longer retention period. At the completion of the retention period, the records must be designated for disposition. This may require records to be transferred to archives, or returned to third-parties, but in many cases, the disposition will be destruction. Duplicates, including extracts from core business systems (eg Campus Solutions, Resource Link, Oracle Financials) must be disposed of as soon as they are no longer needed.
- Disposition of relevant records must be suspended in the event of pending or ongoing litigation or audit. The Directorate of Legal Affairs and Board Secretariat will designate records that are to be held pending resolution of the litigation or audit, and notify all affected staff when the hold is issued and when the hold is released.
- Destruction of records must be performed in a secure manner, ensuring that records to be destroyed are transported securely and destroyed completely in a manner that renders the information completely and irreversibly destroyed.
- For advice on records which may have historical or long term significance, or which are marked for archival assessment on the Retention Schedule, please contact the University Archive and Records Centre.

3.4 Information security classification responsibilities

The following roles and responsibilities have been defined for Information Security classification and are described in more detail in the Information Governance Accountability and Assurance Framework:

- Heads of Schools, Directors or equivalent are responsible for all information processed by their School, Directorate or equivalent.

- The Senior Risk Information Owner ("SIRO") provides leadership for Information Asset Owners through the Information Governance Office and effective networking structures, including engaging with the Information Governance Officers, Guardians and Coordinators, sharing of relevant experience, provision of training and risk reporting.

- The Information Asset Owner:
  - is accountable for the end-to-end lifecycle management of their information;
  - must classify the information for which they are accountable;
  - must annually review its classification and the appropriateness of the controls associated with the information security classification;
  - must make all recipients of information, including third-parties, aware of the minimum control requirements; and
  - must consult the Head of Information Governance where controls beyond those in place for Highly Restricted information are required.

- 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 digital, paper or verbal means, is required to keep the information secure to the level required by the Information Asset Owner and in line with the mandatory minimum protection and security controls for each classification which can be found in the Information Handling Minimum Controls (see Appendix A).

3.5 Incident reporting

If information is lost, stolen, corrupted or disclosed to, or accessed by, unauthorised persons, it must be reported to the Information Governance Office as soon as possible in order that appropriate measures can be taken to contain any damage and minimise the harm which might arise. This includes actual incidents and potential incidents or "near misses".

4 Monitoring compliance with the Procedure

4.1 Enforcement

Heads of Schools, Directors or equivalent are accountable for obtaining assurance that all staff within their area act in accordance with this Procedure.

4.2 Audit

Staff awareness of this Procedure will be audited periodically.

4.3 Reporting

The Head of Information Governance will report on the Procedure to the Information Governance Committee.

5 Review of Procedure

This Procedure will be reviewed every year or when significant changes are required.

6 Contact list for queries related to this procedure

Role	Name	Telephone	email
Head of Information Governance	Tony Brown	0161 306 2106	Tony.Brown@manchester.ac.uk
Deputy Head of Information Governance	Barbara Frost	0161 275 2122	Barbara.Frost@manchester.ac.uk

Version amendment history

Version	Date	Reason for change
1.1	5 May 2017	Minor changes: Information Owner changed to Information Asset Owner; reference to SIRO, IG Office, IG Committee, GDPR; amended definition of information lifecycle; reference to UoM Archives; contacts changed
1.2	11 Jan 2018	Minor changes: removal of reference to DP Act and GDPR; add export controls; change IT Partner to Relationship Manager; review timescale changed to one year – approved by IG Committee 23 Jan 2018
1.3	13 March 2020	Minor changes: renamed directorate; consistency with IG accountability and assurance framework; links to Export Control information

Document control box	
Procedure title:	Standard Operating Procedure – Information Security Classification, Ownership and Secure Information Handling
Version:	1.3
Date approved:	23 Jan 2018
Approved by:	Information Governance Committee
Supersedes:	IT Security Policy: Information Handling, Encryption and Mobile Computing
Next review date:	April 2021
Related Statutes, Ordinances, General Regulations	• Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems • University General Regulation XV Use of Information Systems
Related policies and procedures:	• Information security policy: http://documents.manchester.ac.uk/display.aspx?DocID=6525 • Export of controlled items from the University of Manchester: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=42761 • IG accountability and assurance framework SOP: http://documents.manchester.ac.uk/display.aspx?DocID=8039 • Acquisition, development and maintenance of IT systems, software and/or services: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16369 • Records retention schedule: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514
Policy owner:	Head of Information Governance

APPENDIX A

INFORMATION HANDLING MINIMUM CONTROLS

This guide provides a framework to help manage the confidentiality, integrity and availability of the University's information and supports the Information Security Classification, Ownership and Secure Information Handling SOP. Follow "The Process" to start with and this will refer you to other supporting information within this guide. Contact the Information Governance Office at information.governance@manchester.ac.uk for further advice and guidance.

The Process:

① Create document

② Apply appropriate Protective Marking. Refer to Section A.
All paper-based or digital information created should have a header or footer printed on each page stating the Protective Marking. Most documents will be Unrestricted or Restricted.

③ What do you want to do now?
External sharing: If the document needs to be shared externally then refer to Section B and C
Internal: Refer to Section C

Section A – Which confidentiality classification do I use?

Examples of information in these classifications can be found here: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=15677 with the caveat that the examples are provided as a guide and not a defined list, as the circumstances of each case must be considered in order to assess the harm that might occur to any individuals concerned, or the impact on the University, should there be a breach of confidentiality.

Highly Restricted (High Impact)	Restricted (Medium Impact)	Unrestricted (Low Impact)
Information which if disclosed to unauthorised persons would have a significant adverse impact eg: • Significant distress or financial loss to individuals[1] • Significant fines and enforcement action by the ICO for data breaches; • Significant reputational damage; • Withdrawal of one or more significant research grants or donations; • Litigation against the University; and/or • Significant financial loss due to premature disclosure of IP.	Information that, whilst not classified as Highly Restricted, could result in harm or distress to individuals[1] or the University if there were a breach in confidentiality.	Information where a breach in confidentiality would result in little or no adverse effect on individuals or the University.

[1] For example: students; customers; alumni; applicants; donors; potential donors; parents of current or former students; current, former and prospective employees; research volunteers.

Section B – Sharing information externally

Why?
- Why do I need to provide this information?
- You must understand why the recipient needs access to this data. Disclosure must only be made if you are satisfied that the other person needs it to do their job. If this is not the case or it's unclear, contact the Information Governance Office who will help to confirm if you should share it.

What?
- What are they asking for?
- You must ensure that you only provide the essential data and nothing more and wherever possible you should desensitise it by removing non-essential sensitive data or anonymising the data to obscure the identity of any individuals.

Who?
- Who should I consult before I respond?
- You may need to consult your line manager and/or the information asset owner first. You must never share person identifying information with outside organisations or people, including the police and legal advisers, without first speaking to the Information Governance Office.

How?
- How should I respond?
- Sharing information with third-parties, including UoM associated organisations, may require a signed confidentiality contract or data processing agreement. Seek advice from the Information Governance Office.
- There are recommended routes for sharing information securely - these are outlined on the following page.

Section C – Guide for handling information securely

TYPE	PROCESS	HIGHLY RESTRICTED	RESTRICTED	UNRESTRICTED
Digital information		• Master copies of all UoM information must be stored on University-approved storage (eg UoM data centre). • Portable storage devices must only be used temporarily and must be encrypted where appropriate. • Emails regarding University matters must not be forwarded to personal non-UoM email accounts.		
	General protective measures	• Requires authenticated access (eg UoM login) plus additional access controls (eg specific permissions and privileges) • 2-factor authentication required • Must be encrypted • Must only be accessed using a UoM managed device • Accessible off-campus using VPN • Permissions must be reviewed by the information/service owner at least quarterly	• Requires authenticated access (eg UoM login) plus additional access controls (eg specific permissions and privileges) • Accessible off-campus using VPN • Permissions must be reviewed by the information/service owner at least annually	• Can be used with uncontrolled access eg available on website • Consider converting to PDF to ensure integrity of the document
	Internal transmission incl email	• Must be encrypted (eg encrypted email attachment) and the password conveyed through a different route • Check distribution list carefully • Set a delayed send to enable email errors to be corrected	• Check distribution list carefully • Set a delayed send to enable email errors to be corrected • Encryption may be recommended by the Information Owner	• Set a delayed send to enable email errors to be corrected
	External transmission/ collaboration	• Refer to Section B – sharing information externally • Obtain permission from the Information Owner • Must be encrypted	• Refer to Section B – sharing information externally • Must be encrypted if emailed to a non-University email account	• Set a delayed send to enable email errors to be corrected
	Disposal	• Delete files then delete from recycle bin • Contact IT Services for advice on disposal of device if required	• Delete files then delete from recycle bin • Contact IT Services for advice on disposal of device if required	• Normal deletion and reuse
Paper information	General protective measures	• Avoid printing • Protect by a minimum of 2 physical locks eg locked office and locked storage • Must not be removed from UoM premises • Consider scanning and send as encrypted email attachment	• Avoid printing • Protect by 1 physical lock eg locked storage • Consider scanning and sending as email attachment	• Freely accessible
	Internal circulation	• Request specific hand delivery • Use double envelope ie sealed unlabelled outer envelope, inner envelope labelled “Highly Restricted”	• Use sealed envelope – do not mark as “confidential” or similar on the envelope	• Re-usable envelopes
	External circulation/ collaboration	• Use “Track and trace” or similar service which requires signature on receipt • Use double envelope – only the inner envelope should be labelled “Highly Restricted”	• Standard postal service • Do not mark as “confidential” or similar on the envelope	• Standard postal service
	Disposal	• Use local cross-cut shredding machine or lockable bins provided by University-approved on-site shredding suppliers	• Use local cross-cut shredding machine or lockable bins provided by University-approved on-site shredding suppliers	• Recycle in blue bags provided by Estates