Standard Operating Procedure

Title:	Information Security Classification, Ownership and Secure Information Handling		
Version:	1.4	**Effective Date**	March 2022
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 of interest, and increasingly at risk, due to ever-expanding and capable cyber security threats, alongside the business imperative to share information internally and with outside organisations and individuals.

The use and safeguards required of some information is constrained by contracts, legislation, current research funders, Data Protection and Export Control Joint Unit legislation, or in order to protect the interests of the University, whilst other information may need to be made freely available[1], such as information in response to Freedom of Information legislation requests and open research.

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 and fully standardised security controls 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 improve the handling and treatment of confidential information in the University by:

- Establishing key/baseline information security classifications for University information;
- Providing guidance for Information Owners in applying information security classifications;
- Ensuring that appropriate baseline controls are applied which are commensurate with the selected information security classification;
- Providing appropriate information handling instructions commensurate with the selected information security classification; which will
- Minimise the University's exposure to information risk and potential negative impacts on the operation of the University, financial loss, reputation damage or legal proceedings arising from a breach of the confidentiality of information.

Classifying information is a foundational step towards the development of more secure systems where appropriate "first line of defence" security controls are automatically applied.

[1] 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

This Procedure does not attempt to describe the environments (systems, technology) which are suitable for processing information in each classification. General guidance on the use of University systems which are widely used for storing and sharing information can be found on the Information Governance Office website.

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. 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. 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 Processing Activity Owners.

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).

Personal data includes information from which an individual can be identified directly from the information or indirectly in combination with other information. Further information is available on the Information Commissioner's Office website https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/

Information Security involves consideration of the following aspects as mitigation, particularly in the context of significant cyber threats:

- **Confidentiality** – concerned with preserving authorised restrictions on information access and disclosure, including the protection of personal data 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.

The primary focus of this Procedure is on **Confidentiality** and the underpinning requirement to ensure that information is only accessed by those authorised to do so. There are specific techniques to mitigate integrity risks (such as secure signing and hashed data) and to mitigate availability risks (such as backups and mirrored systems) and access controls are fundamental to mitigating these risks too.

Any reference to information security classification labels will be shown in capitals eg VERY SENSITIVE, HIGHLY RESTRICTED, RESTRICTED, UNRESTRICTED.

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 teaching, research, administration other activities 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 and accessed 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 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.

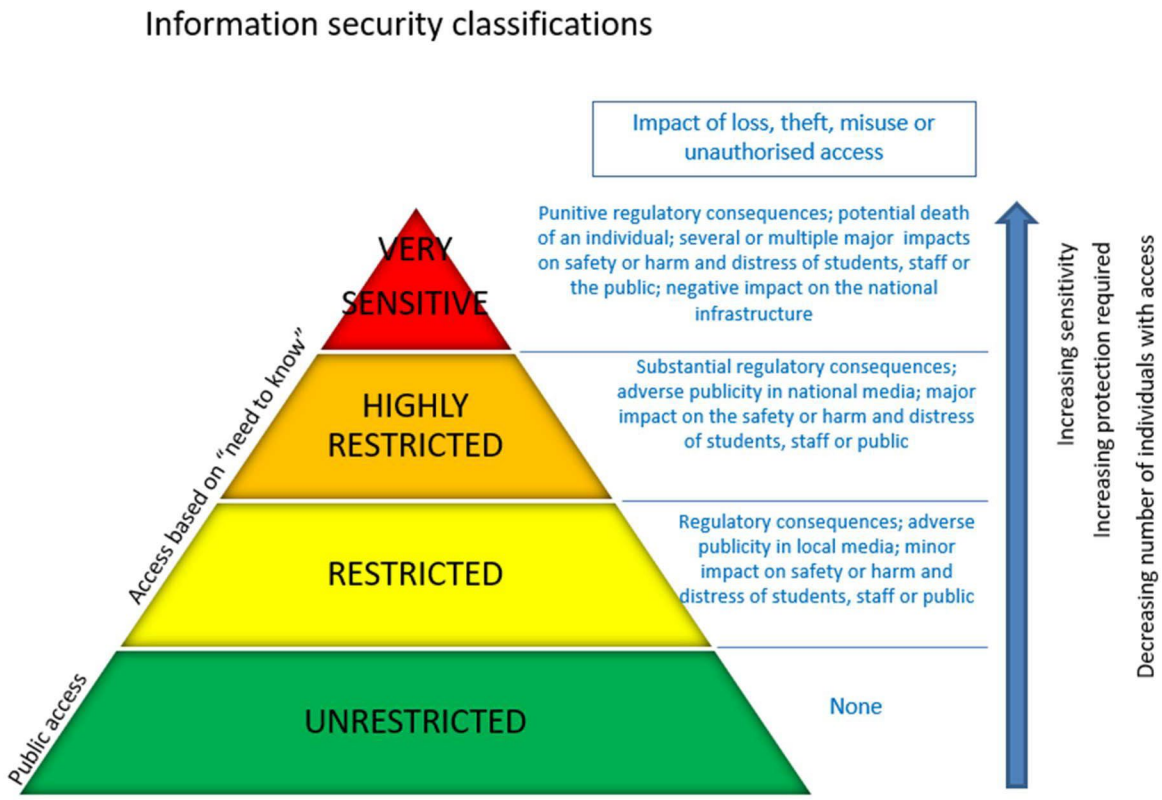
- **All authorised users** of information are responsible for its safe custody. Anyone who has access to information whether as a user of a software application or as a recipient of information via digital, paper or verbal means, is required to keep the information secure to the level required by the Information Asset Owner and in line with the mandatory minimum protection and security controls for each classification

All information processing should consider:

- What the **impact** would be if the information was lost, stolen, misused or accessed by unauthorised individuals (see Section 3.3)
- How the **likelihood** of such an event can be minimised (see Section 3.4)

3.3 Information security classification - impact assessment

3.3.1 The information security classification is determined by assessing the adverse impact or damage that would occur if information were to be lost, stolen, misused or accessed by unauthorised individuals. The impact is aligned to the University's risk management impact levels (see Appendix A) and the information security classification helps to determine the appropriate level of protection for the information (see Section 3.4).



Where the impact is assessed as "serious", "major" or "catastrophic" this might mean that the information should be classified as VERY SENSITIVE and enhanced security is required (see Section 3.4). Advice must be sought from the University's Head of Information Governance and/or the Research Relationship Oversight Group in such circumstances **before** any contracts are signed or data is obtained.

3.3.2 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 because the impact of disclosure has become minor eg University financial statements and research papers before and after publication;
- **Volume of data** - For example, several data sets which separately might be classified as RESTRICTED, when brought together may have a potentially higher adverse impact and would be classified as HIGHLY RESTRICTED; the personal data of one individual which would normally be

classified as RESTRICTED, may need to be classified as HIGHLY RESTRICTED where the records of hundreds of people are involved because the impact of disclosure could have serious regulatory consequences;

- **Context** – For example personal data which might normally be classified as RESTRICTED may be categorised as HIGHLY RESTRICTED if it belongs to someone whose physical safety is at risk;
- 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.

3.3.3 Examples of information in each classification can be found in the "Information Security Classification Examples and Handling Guidance",

3.4 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, who is involved in the collaboration, how it is disposed of. Information should only be shared on a need-to-know basis. 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 and common-sense precautions to limit access but must also be balanced with ease of access required by authorised users.

The mandatory minimum protection and security controls for HIGHLY RESTRICTED and RESTRICTED information can be found in the "Information Security Classification Examples and Handling Guidance".

In exceptional cases where more restrictive protection is required than described in the "Information Security Classification Examples and Handling Guidance", advice must be sought from the University's Head of Information Governance and/or the Research Relationship Oversight Group before any contracts are signed or data is obtained. This includes for example:

- information classified as VERY SENSITIVE
- collaborations with industry or UK Government departments which may require specific security classifications and security arrangements to be put in place eg individuals may require security clearance to handle information; individual environments for specific work packages may be required for research activities such as Turing tier 3/4 environments. The approximate alignment of the University's classification scheme with UK Government and Turing guidance is shown in Appendix B and C respectively.
- NHS collaborations where the data involved does not meet the criteria for storage in the University's Data Safe Haven (which has enhanced security arrangements in relation to specific NHS contracts)
- where the likelihood of a **targeted** attempt to access HIGHLY RESTRICTED 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

3.4.1 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.

- Information classified as VERY SENSITIVE requires enhanced security to be determined with the Head of Information Governance and/or the Research Relationship Oversight Group.
- 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 at rest and/or in transit, including data on University systems and with third-party/cloud service providers.

3.4.2 Protective marking and labelling

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 should involve displaying the sensitivity marking (eg UNRESTRICTED, RESTRICTED, HIGHLY RESTRICTED, VERY SENSITIVE) in the file name, somewhere on each page of a document or using Sensitivity Labels for Microsoft 365 Office documents if available. Additional handling instructions may also be provided eg "Do not distribute this document further".

All HIGHLY RESTRICTED and VERY SENSITIVE information **must** be protectively marked.

Core business applications which process HIGHLY RESTRICTED and RESTRICTED information do not require labelling but must be compliant with the controls relevant to the classification as described in the Technical Security Standards.

When working with Government OFFICIAL-SENSITIVE information, the Government label must be applied in addition to the HIGHLY RESTRICTED or VERY SENSITIVE label but adhering to the handling instructions provided by the Security Aspects Letter or other Government instructions, where they are more restrictive than those required for University information.

3.4.3 Sharing and collaborating - principles

Whenever information is shared or worked on jointly within the University or with partners and collaborators, the exposure to risk increases.

VERY SENSITIVE information would not normally be shared with external partners and, where third-party organisations do share their VERY SENSITIVE information with the University, they will often insist that University staff use their systems. Advice must be sought from the University's Head of Information Governance and/or the Research Relationship Oversight Group in such circumstances **before** any contracts are signed or data is obtained, and before any VERY SENSITIVE information is shared.

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
- 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;
- 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;

- Usually there will be a contract in place to share HIGHLY RESTRICTED or RESTRICTED information with a third-party. However, where ad hoc requests for personal data are received from third-parties (eg from the Police or external legal advisers), the personal data must not be shared without first consulting the Information Governance Office;
- Where appropriate, a retention period and mechanism for disposal and audit should be agreed with the third-party;
- Export controlled information must only be shared in accordance with the relevant University guidance on Export Control – 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 include a Data Processing Agreement and 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.

All documents created using Microsoft Office 365 (Outlook, Word, Excel, PowerPoint) must be given a sensitivity label, where available, and should be shared by providing links to the documents which are stored in OneDrive or SharePoint, wherever possible, in order to reduce the volume of documents in circulation and to make use of the access controls which links can provide.

3.4.4 Document lifecycle management

The Document and Information Management Standard Operating Procedure describes the various procedures for ensuring that documents on University systems are managed according to appropriate standards across their entire lifecycle. The Records Retention Schedule describes the time periods for which records should be retained by the University in order to comply with operational and legal requirements, including data protection legislation.

University information, apart from information classified as UNRESTRICTED, which is not required to be kept in accordance with the Records Retention Schedule, must be securely destroyed using University-approved methods.

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 infosec@listserv.manchester.ac.uk 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 including metrics regarding the application of protective marking and labelling.

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
1.4	8 March 2022	Addition of Very Sensitive classification; emphasis on impact of unauthorised disclosure; mandatory marking for Highly Restricted and Very Sensitive information.

Document control box	
Procedure title:	Standard Operating Procedure – Information Security Classification, Ownership and Secure Information Handling
Version:	1.4
Date approved:	8 March 2022
Approved by:	Information Governance Committee
Supersedes:	IT Security Policy: Information Handling, Encryption and Mobile Computing
Next review date:	April 2023
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

	• Document and Information Management SOP https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=45530 • Records retention schedule: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514
Policy owner:	Head of Information Governance

APPENDIX A

Alignment of information security classifications with impact levels

University Strategic Risk Register impact assessment	NO RISK	MINOR	MODERATE	SERIOUS	MAJOR	CATASTROPHIC
	No financial loss	Financial loss less under £10M	Financial loss between £10M-£20M	Financial loss £20M - £50M	Financial loss £50M - £100M	Financial loss >£100M
Regulatory and reputational impact	No regulatory consequences	Regulatory consequences; adverse publicity in local media	Substantial regulatory consequences; adverse publicity in national media	Punitive regulatory consequences; negative impact on the national infrastructure		
Impact on individuals	No impact	Minor impact on the safety or harm and distress of students, staff or the public	Major impact on the safety or harm and distress of students, staff or the public	Potential death of an individual; multiple major impacts on safety or harm and distress of students, staff or the public		
UoM information security classification	UNRESTRICTED	RESTRICTED	HIGHLY RESTRICTED	**VERY SENSITIVE Contact the Head of IG[1] or Research Relationship Oversight Group[2] prior to starting to process this data as enhanced security may be required**		

[1] email: information.governance@manchester.ac.uk

[2] Research Relationship Oversight Group

'APPENDIX B

Approximate alignment with UK Government classification scheme

<table>
<tr><td rowspan="2">UK Government classification scheme</td><td>OFFICIAL</td><td colspan="2">OFFICIAL - SENSITIVE (or other suffix and descriptor)</td><td>SECRET</td><td>TOP SECRET</td></tr>
<tr><td>Not subject to heightened threat profile; the level of confidentiality needed to protect an asset, covering the majority of government work</td><td>Potentially subject to heightened threat profile;</td><td>If the information owner has specified enhanced security measures this may align with VERY SENSITIVE UoM classification</td><td>Information subject to a heightened threat profile requiring protective measures to defend against determined and highly capable threat actors</td><td>Information requiring the highest levels of protection from the most serious threats.</td></tr>
<tr><td>UoM information security classification</td><td>RESTRICTED</td><td>HIGHLY RESTRICTED</td><td>VERY SENSITIVE</td><td colspan="2">UoM is not normally permitted to process SECRET OR TOP SECRET government information as the University does not have List X clearance and staff require security clearance in order to process this data</td></tr>
<tr><td colspan="6">However, the controls required in these environments may not directly align with the controls currently in place at UoM and advice must be sought from the Head of Information Governance where Government contracts require specific controls</td></tr>
</table>

APPENDIX C

Approximate alignment with Turing Data Safe Haven tiers

Turing Data Safe Haven tiers	**Tier 0 environment**	**Tier 1 environment**	**Tier 2 environment**	**Tier 3 environment**	**Tier 4 environment**
	Publicly available data; data intended for immediate publication	Data intended for eventual but not immediate publication; data sets where the only risks of disclosure are to the researchers' competitive advantage; pseudonymised or synthetic data where confidence in the quality of anonymisation is absolute; commercial information where the consequences of disclosure are so low as to be trivial	Pseudonymised or synthetic data where confidence in the quality of anonymisation is strong; commercial data where risks from disclosure are low; very unlikely to be subject to targeted attack	Pseudonymised personal data where confidence in the anonymisation is weak; commercial data which is sensitive; Information which could be subject to attack by attackers with bounded capabilities such as hackers	Personal data where disclosure poses a substantial threat to safety, security or health; commercial or governmental data which could be subject to attack by sophisticated, well-resourced and determined actors such as nation states
UoM information security classification	UNRESTRICTED	RESTRICTED		HIGHLY RESTRICTED	VERY SENSITIVE
However, the controls required in these environments do not directly align with the controls currently in place at UoM and advice must be sought from Research IT					