MANCHESTER 1824
The University of Manchester

Standard Operating Procedure

Title	Information Security and Data Protection Incident Reporting		
Version	1.5	Effective Date	March 2020
Summary	Describes the procedure for reporting information security incidents to the Information Governance Office		

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 https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=15678 for any new versions.

1 Background and purpose

The University has implemented a number of technical and procedural controls and staff training to help protect the University's information from a breach in the confidentiality, integrity or availability of the information. Where these measures fail, either deliberately or accidentally, the requirements of this Procedure must be followed.

The purpose of this Procedure is to ensure that all actual and potential information security incidents are reported in order to:

- facilitate a fast response to incidents in order to contain or minimise the impact of the incident;
- clarify the responsibilities of those involved in reporting incidents;
- provide support to those who are affected by the incident; and
- provide information regarding the causes of incidents so that improvements can be made to mitigate the risk of a further occurrence.

Reporting of incidents and "near misses" should be viewed positively as it will allow the University to analyse trends, rectify vulnerabilities and thereby reduce the likelihood or impact of future incidents.

2 Definitions and scope

For the purpose of this Procedure the following definitions apply:

Highly Restricted and Very Sensitive Information – the unauthorised or accidental disclosure of this type of information would result in a significant financial, regulatory, reputational or legal impact on the University. Examples of information which fall into these categories can be found here.

Information – means 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 data, the manual or automated systems that process it, the methods by which it is distributed or the locations from which it is accessed.

Information Security Incident – is an event which results or has the potential to result in the compromise, misuse, or loss (confidentiality, integrity or availability) of information or information assets at the University, including actual or suspected incidents, as well as any perceived weaknesses that may cause an incident to occur. A Data Protection Incident includes person-identifying information. Incidents include, for example:

- Confidentiality losses:
    - the accidental or deliberate unauthorised disclosure of information, such as person-identifying information;
    - the unauthorised access to information or systems;
    - the theft of information systems/equipment or data;
    - breach of policy - such as the Information Security Policy or Data Protection Policy
- Integrity losses:
    - the accidental or unauthorised deliberate modification of information;
    - the incorrect processing of data.
- Availability losses:
    - the accidental or unauthorised deliberate destruction of information;
    - actions which make an information system unavailable;
    - the inability to access an information system when needed for operations

Further examples are listed in Appendix A.

Person-identifying information - any data which relates to a living individual who can be identified from that data, or from that data in conjunction with other readily available information.

Special category and criminal conviction personal data (previously known as Sensitive Personal Data): a sub-category of personal data that could cause harm or distress to an identifiable individual if generally released, including information relating to an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification)
- Health
- Sex life or sexual orientation
- Criminal convictions and offences

Additional conditions and safeguards must be applied to ensure that special category and criminal conviction personal data is handled appropriately by the University and is treated as Highly Restricted information. The University also recognises other personal data besides special category data as Highly Restricted information. Other examples can be found here.

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 IT facilities ("staff"). This includes temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the University and suppliers (this list is not intended to be exhaustive). This Procedure also applies to students who have access to information classified as Very Sensitive, Highly Restricted or Restricted or critical systems, related to the conduct of University matters, such as University-led research.

NB – Where the incident relates to the loss or potential loss of payment card data, then the process as outlined in the PCI DSS Incident Response Management SOP must be followed.

3 Procedure and responsibilities

3.1 Consequences 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.

3.2 Report and contain potential harm

All information security incidents must be reported to the Information Governance Office ("IGO") as a matter of urgency and if the incident involves Very Sensitive or Highly Restricted Information, such as special category or criminal conviction personal data or a large volume of person-identifying information, you must contact the IGO immediately. This is so that the seriousness of the incident can be assessed as soon as possible and advice can be provided on any immediate containment action required to minimise the impact.

Information Governance Office	Tel: 0161 275 7789 or email: infosec@listserv.manchester.ac.uk

Staff must not attempt to manage information security incidents themselves. This includes both positive and negative actions: do not attempt to modify, limit or contain the extent of the incident unless explicitly instructed to do so by the IGO.

Where an incident occurs outside office hours and the incident involves actual or immediately threatened harm to individuals, contact the Security Office who will inform the Emergency Incident Manager on your behalf.

Security Office	Tel 0161 306 9966 (the number is on the back of all staff/student ID cards

If in doubt, it is better to report a suspected incident than to ignore it.

3.3 Investigate and assess risks

3.3.1 Information gathering

Staff must co-operate promptly with the IGO to gather information relating to the scope of the incident. This includes completing the incident report as quickly as possible.

If it is concluded that a serious or complex incident has occurred, an Information Security Incident Response Team may be set up, comprising appropriate University expertise to manage the incident.

3.3.2 Confidentiality

Any discussion of the incident or circulation of any related documents or emails must be restricted to those directly involved in the investigation.

3.4 Actions and notifications

3.4.1 Any further actions to be taken will be determined following the investigation.

3.4.2 The communication of any data breach which involves person-identifying information must be handled with care and sensitivity, and appropriate advice will be provided.

3.4.3 Wider communication of an incident, including notification to any regulatory authorities, such as the Information Commissioner's Office or research sponsors, will be managed by the Information Security Incident Response Team.

3.5 Incident evaluation and follow up

The incident may highlight remedial action which is required in relation to procedures, IT systems or the incident reporting procedure. Any agreed actions and target dates for completion will be recorded. The Information Governance Office will:

- liaise with the Information Governance Guardian to ensure that local actions are completed;
- escalate any actions which have not been completed by the target date; and
- ensure that guidance material is revised to reflect any learning outcomes.

4 Monitoring compliance with the Procedure

4.1 Enforcement

Heads of School, Directors or equivalent are responsible for ensuring 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 provide a report on this Procedure to the Information Governance Committee. A summary report will be provided comprising:

- the number and type of incidents raised; and
- the key factors giving rise to the incidents and possible mitigation to prevent further occurrence.
- any lessons learned to improve the Procedure.

Any significant incidents will be reported to IGC at their quarterly meetings.

5 Review of procedure

This Procedure will be reviewed at least every two years 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
Head of Data Protection	Callum Lyons		Callum.Lyons@manchester.ac.uk
Head of Information Security	Eddie Hill		Eddie.hill@manchester.ac.uk

Version Amendment History

Version	Date	Reason for change
1.0	October 2017	Creation – (IG Sub-committee 9 Oct 17); approved by IGC 23 Jan 18
1.1	December 2017	Url changed to incident form
1.2	January 2018	Amended for GDPR; minor changes plus Special Category data definition added/amended
1.3	23 Jan 2018	Changed Special Category data list to be consistent with Data Protection Policy as requested by HOIG
1.4	16 March 2020	Minor changes: Link to Highly Restricted examples added; link to incident form removed
1.5	27 May 2022	Added Very Sensitive classification; change of contact details

Document Control

Procedure title:	Information Security and Data Protection Incident Reporting Standard Operating Procedure
Date Approved	May 2022
Approving Body	Information Governance Committee – minor change approved by HoIG
Version	1.5
Supersedes	1.4
Previous Review Dates	N/A
Next Review Date	March 2024
Related Statutes, Ordinances & General Regulations	
Related Policies	• Data Protection Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914 • Information Security Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525
Related Procedures	• Information classification, ownership and secure information handling SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 • Acceptable Use SOP for Staff: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 • Acquisition, Development and Maintenance of IT Systems and/or Services SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16369 • PCI DSS Incident Response Management SOP: http://documents.manchester.ac.uk/display.aspx?DocID=29831
Related guidance and or codes of practice:	• Information security classification examples - confidential information: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=15677
Related Information	
Procedure Owner	Head of Information Governance

APPENDIX A

EXAMPLES OF INFORMATION SECURITY INCIDENTS

The examples provided below are a guide and not a defined list.

- Actual unauthorised disclosure of Very Sensitive, Highly Restricted or Restricted information[1] for example:
    - by sending an email or Teams chat/post to the wrong internal or external recipient
    - by attaching incorrect attachments to emails
    - by including data in the attachment or in the thread of the email which shouldn't be provided
    - uploading information to to a website which can be accessed by unauthorised persons
    - uploading information to a SharePoint site which should not be available to those who have access to the site
    - sharing a sharepoint link outside the security classification including need to know
    - including live data in testing or training materials
    - papers collated incorrectly and sent to an incorrect recipient
    - phishing/ransomware
- Potential disclosure of Very Sensitive, Highly Restricted or Restricted information[1] for example information in digital, paper or other format which is:
    - held in unlocked cabinets/cupboards
    - missing from archives, cupboards, desks, printers
    - left on desks, printers, whiteboard or flipchart displays in meeting rooms
    - left, lost or stolen - for example:
        - stolen from premises or cars
        - left on public transport
        - lost in transit
        - left behind during office removals
    - incorrectly disposed of eg papers not shredded on disposal or left in insecure locations prior to shredding; digitally stored information not securely wiped
- Lost or stolen equipment which provides access to University information for example:
    - Laptops, desktop PCs, teaching PCs, tablets, removable storage devices such as USB sticks and removable hard drives
    - University issued or supported smart phones
- Technical Incidents
    - Backup failure
    - Unplanned system downtime
    - Patch management process failure
- Unauthorised access to University buildings where information may be at risk
- Unauthorised access to information through a failure to ensure
    - clearance
    - vetting
    - export control personnel restrictions
- Breach of University procedures which are intended to protect the University's information and information systems for example:
    - the Acceptable Use SOP for Staff prohibits password sharing, storing unencrypted person identifying data on non-University IT facilities, failing to adhere to software

[1] Further examples of information in these classifications can be found: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=15677

development standards, introducing malware, attempting to access information without authorisation.

- the Acquisition, Development and Maintenance of IT Systems and/or Services SOP requires that an Information Governance Risk Review must be undertaken prior to the commissioning of any new system.
- the Information Security Classification, Ownership and Secure Information Handling SOP stipulates baseline security requirements for Very Sensitive, Highly Restricted and Restricted information