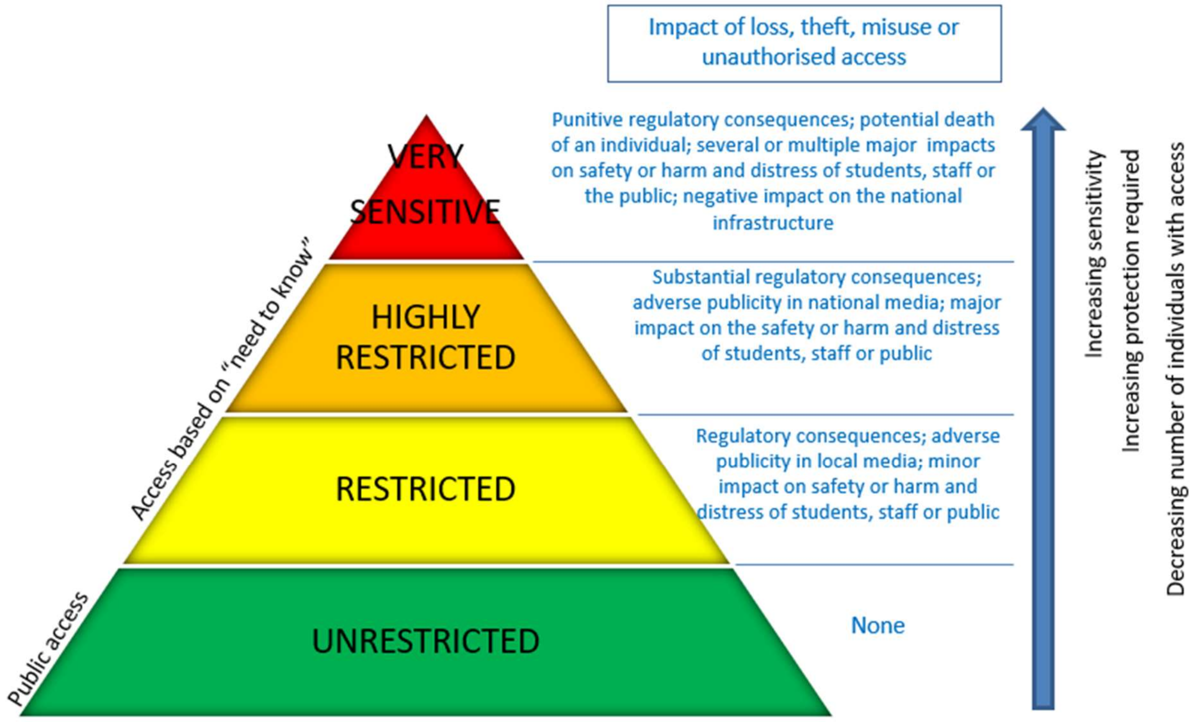
INFORMATION SECURITY CLASSIFICATION EXAMPLES AND HANDLING GUIDANCE

The University is publicly accountable and the principles of openness, transparency and information reuse require individuals to consider proactively publishing information. However, this must be a reasoned judgement, taking data protection, confidentiality and information which should only be shared on a "need-to-know" basis into account - such information should be given an information security classification which 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. Section 1 below provides examples of information in the University's classification scheme and section 2 provides a guide to the type of protection which should be used. However, these are only examples, as the impact, and therefore the way the information is handled, may vary depending on the context.

Information security classifications


Impact of loss, theft, misuse or unauthorised access
VERY SENSITIVE
Punitive regulatory consequences; potential death of an individual; several or multiple major impacts on safety or harm and distress of students, staff or the public; negative impact on the national infrastructure
HIGHLY RESTRICTED
Substantial regulatory consequences; adverse publicity in national media; major impact on the safety or harm and distress of students, staff or public
RESTRICTED
Regulatory consequences; adverse publicity in local media; minor impact on safety or harm and distress of students, staff or public
UNRESTRICTED
None
Access based on "need to know"
Public access
Increasing sensitivity
Increasing protection required
Decreasing number of individuals with access

1 Information Security Classification examples

The examples provided below are 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[1] concerned, or the impact on the University. If you wish to add more examples, or have any comments or queries, please contact information.governance@manchester.ac.uk.

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

VERY SENSITIVE	• Impact if lost, stolen, misused or accessed by unauthorised individuals eg negative impact on the national infrastructure; punitive regulatory consequences; potential death of an individual ; multiple major impacts on safety or harm and distress of students, staff or the public; • For use by a tightly controlled group of users who may need security clearance • 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
Research relating to: • Security sensitive material eg commissioned by military, requiring a Security Aspects Letter; involves acquisition of security clearance; concerns terrorists or extreme groups; relates to human rights violations • Work packages which require specifically enhanced security arrangements (eg Turing level 3/4 research environments) Passwords to University systems must NEVER be disclosed to ANYONE	Research related to University "Research Beacons" and other key industrial fields **at particular risk of being targeted by foreign states**: [2] Energy conservation and environmental protection industries: • Nuclear technologies • Energy efficiency • Advanced environmental protection industries • Resource recycling industries Next generation technology: • Next generation information networks • Core basic electronics industries • High-end software and emerging information service industry Bio-industry: • Biomedical • Biomedical engineering • Biological agriculture industry • Bio-manufacturing High-end equipment manufacturing industries: • Aviation equipment • Satellite and applied industries • Marine engineering • Rail transport equipment • Smart manufacturing equipment industries New energy: • Nuclear technologies • Wind energy • Solar • Biomass New materials: • New functional materials • Advanced structural materials • High performance composites New energy vehicles: • Purely electric • Hybrid powered

[2] Source: Universities UK: Cyber Security and Universities - Managing the risk; NCSC: The cyber threat to Universities

HIGHLY RESTRICTED	• Impact if lost, stolen, misused or accessed by unauthorised individuals eg substantial regulatory consequences; major impact on the safety or harm and distress of students, staff or the public; adverse publicity in national media • For use by a tightly defined group of users and deals with issues that they are exclusively authorised to handle
Sensitive personal data (defined as Special Category data by Data Protection law) consisting of information as to: • race or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data (where used for identification purposes) • health • sex life or sexual orientation This includes photographs which in some circumstances can indicate ethnicity or religious beliefs. Personal data relating to criminal convictions and offences. Any personal data belonging to people whose physical safety is at risk eg: • People under the direct threat of violence eg victims of domestic violence, individuals involved in politically sensitive subject areas or research areas • Celebrities, notorieties and VIPs including those who publicly promote controversial views • People in security-sensitive roles • Individuals at risk of serious self-harm	Information that links one or more identifiable living persons with information about them which, if released would put them at significant risk of harm or distress eg: • Financial information eg salary, National Insurance Number, bank account details, tax, benefit or pensions records, debt information • Credit or debit card details – NOTE: these must not be recorded ANYWHERE on UoM systems (apart from University-owned accounts) and if provided to the University they must be destroyed or deleted as soon as possible • Passport number • The complete staff/student record for an individual • Material related to social services including child protection • Mitigating circumstances • Disciplinary proceedings • Preliminary degree classification/transcript information pending formal approval and publication
• Any information which is subject to contractual constraints • Information related to items subject to export control including emails or other documentation – see Export Control website • Commercially valuable intellectual property • Information which may be regarded as highly commercially sensitive	• Legal advice and other information relating to legal action against or by the University • Information which relates to University security matters • Reserved committee papers • Restricted personal datasets involving several hundred data subjects which may or may not be in the public domain • Risk registers

RESTRICTED	• Impact if lost, stolen, misused or accessed by unauthorised individuals eg regulatory consequences; minor impact on the safety or harm and distress of students, staff or the public adverse effect on individuals or the University; adverse publicity in local media • Intended for use by legitimate groups of University users on a need-to-know basis and rarely of any wider interest
Data that links one or more identifiable living person with information about them which, if released would reveal information about the individual's private life, which may or may not be in the public domain eg • Home address • Home or private mobile telephone numbers • Date of birth • Driving licence number (because shows date of birth and part of surname) • Names of family members or relationships • Postcode • Attendance records	• Question papers and other assessment material prior to an unseen assessment • Routine financial information • Policy and planning documents prior to publication • Key organisational or personnel changes prior to any consultation process • Teaching material including VLE content • Most research records and information prior to publication • Information provided in confidence or under legal privilege • Library electronic resources • Software licences negotiated by the University
Routine records related to staff and students eg • Staff/student ID numbers and usernames – Note: passwords to University systems must NEVER be disclosed to ANYONE • Student directory (names, email addresses, and School) • Course assessments • Student transcripts • Exam scripts • Exam marks • Examiners comments on a student performance • References for staff and students (unless it contains data classified as HIGHLY RESTRICTED) • UCAS forms (unless it contains information classified as HIGHLY RESTRICTED)	• Committee papers prior to a meeting (unless contain Highly Restricted content) • Internal/external audit reports (unless contain Highly Restricted content) [Restricted personal datasets involving several hundred data subjects which may or may not be in the public domain must be treated as HIGHLY RESTRICTED]

Unrestricted	• Impact if lost, stolen, misused or accessed by unauthorised individuals - no adverse effect on individuals or the University; • Intended to reach most staff and/or students and deals with issues that affect them and their day-to-day interactions with the University
Internal - of limited interest to an external audience	
• Staff directory – including where they have opted out of the public list • Exam and meeting timetables • Information made available to the student body as a whole	• Room booking information • Internal circulars, notices, briefings and guidelines
External	
• Staff directory (including names, job titles and work contact details) unless they have opted not to make these available outside the University • Organisation structure (without names) • Publications by staff • Personal data which has been anonymised • Data agreed by data subjects to be put into the public domain • Annual reports	• Financial statements • Important committee records • Other information required to be published under Freedom of Information law • Final degree classification • Information that is publicly available eg from the Office for Students • Information about individuals available through social networking sites where the information is provided to the public

2 Information handling minimum controls

The controls for information classified as VERY SENSITIVE will vary depending on the specific requirements of each case and will be more restrictive than those required for Highly Restricted information. 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.

General guidance on the use of University systems widely used for storing and sharing information can be found on the Information Governance Office website. Researchers should also refer to guidance provided by Research IT and the Library.

HIGHLY RESTRICTED and RESTRICTED information must only be shared on a "need to know" basis and usually there will be a contract in place to share HIGHLY RESTRICTED or RESTRICTED information with a third-party.
There are no specific handling requirements for UNRESTRICTED information.

PROCESS	**HIGHLY RESTRICTED**	**RESTRICTED**
Digital information		
General protective measures	• Users are authenticated through an authentication service provided by IT Services (eg UoM IT account login) plus additional access controls (eg specific permissions and privileges) • Requires 2-factor authentication • Permissions must be reviewed by the information/service owner at least quarterly	• Users are authenticated through an authentication service provided by IT Services (eg UoM IT account login) plus additional access controls (eg specific permissions and privileges)

PROCESS	HIGHLY RESTRICTED	RESTRICTED
	• File must be protectively marked eg using M365 sensitivity labels, in the email subject, filenames, document headings. Additional handling requirements may also be specified eg "Do not distribute this document further"; "For named recipients only" • Must be encrypted at rest and/or in transit • Must only be accessed using a UoM managed device or a trusted device eg mobile device management such as Intune	• Permissions must be reviewed by the information/service owner at least annually
Internal transmission including email and Teams meetings and chats	• Links to files in SharePoint/OneDrive must specify "Specific People" who are allowed access and downloads must be blocked • Email attachments should be avoided where possible (use links instead) otherwise the attachment must be encrypted and the password conveyed through a different route eg SMS or telephone NOT simply a different email • Check distribution list carefully • Set a delayed send to enable email errors to be corrected	• Links to files in SharePoint /OneDrive must specify "People in The University of Manchester with the link" • Check distribution list carefully • Set a delayed send to enable email errors to be corrected
External transmission/ collaboration including email and Teams meetings and chats	• Should only be shared on an "need to know" basis. • Usually there will be a contract in place to share HIGHLY 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 • Obtain permission from the Information Owner • Links to files in OneDrive must specify "Specific People" who are allowed access and downloads must be blocked • Email attachments must be encrypted and the password conveyed through a different route ie SMS or telephone NOT simply a different email • Some information which is subject to Export Control legislation may be prohibited from being accessed outside the UK – see Export Control website	• Should only be shared on an "need to know" basis. • Usually there will be a contract in place to share 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
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
Non-digital eg paper		
General protective measures	• Avoid printing and keep a clear desk, especially if desk areas are shared • Protect by a minimum of 2 physical locks eg locked office and locked storage • Must not be removed from UoM premises • Consider scanning and storing on SharePoint instead	• Avoid printing • Protect by 1 physical lock eg locked storage • Consider scanning and storing on SharePoint instead

PROCESS	HIGHLY RESTRICTED	RESTRICTED
Internal circulation	• Request specific hand delivery • Use double envelope ie sealed unlabelled outer envelope, inner envelope labelled "Highly Restricted" • Consider scanning and send as a SharePoint link (see above)	• Use sealed envelope – do not mark as "confidential" or similar on the envelope • Consider scanning and send as a SharePoint link (see above)
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
Disposal	• Use local cross-cut shredding machine or lockable bins provided by University-approved on-site shredding suppliers NOT recycling bins	• Use local cross-cut shredding machine or lockable bins provided by University-approved on-site shredding suppliers NOT recycling bins

Version amendment history

Version	Date	Reason for change
9	June 2021	Updated link to export control web site
10	March 2022	Added Very Sensitive classification; merged with Information Handling Minimum Controls; Approved by IGC 8 March 2022