The University Of Sheffield.

Information Classification & Handling

What's the Purpose of this Classification Scheme?

All information that the University creates, receives and shares has value. Information Classification is the process of separating information into relevant categories, based on the content of the information and the risks of mishandling or sharing it inappropriately. By identifying the appropriate Classification it is possible to put in place controls and guidance on the best way to create, share, manage and protect the information.

This classification system is in place to make it easier for you to understand what data you need to be careful with.

The implementation of Information Classification helps to build a positive culture of Information Management and security awareness. It puts the responsibility of protecting information on everyone who handles it, and it ensures that all University staff, students, researchers and other affiliates, understand the value of the information they work with on a daily basis, and know how to treat it.

Classification Scheme

As outlined below, the University of Sheffield uses 4 separate classifications for all the information it handles and processes. These are as follows:

Public Information:

Data that if lost, stolen, misused or corrupted would have no negative impact on individuals or the University.

May be viewed by anyone inside or outside the University.

Internal Information:

Data that if lost, stolen, misused or corrupted would have a conspicuous but minor negative impact on individuals or the University.

Available to authenticated users at the University such as staff, research students or students.

Restricted Information:

Data that if lost, stolen, misused or corrupted would have a significant negative impact on individuals or the University.

Only accessible to a specific group/s of people that are granted permission with approval. The permissions are regularly reviewed and updated. The “principle of least privilege” is followed at all times: Users only have the bare minimum permissions they need to perform their work.

Highly Restricted Information:

Data that if lost, stolen, misused or corrupted would have major negative impact on individuals or the University

Access is restricted to a small number of people. The list is regularly reviewed and updated. The “principle of least privilege” is followed at all times: Users only have the bare minimum permissions they need to perform their work.

Classification Scheme Table

Classification	Public	Internal	Restricted	Highly Restricted
Definition	Information publicly available to anyone both inside and outside of the university.	Information only available to users within the University such as staff, contractors and students.	Information only accessible to specific individuals that have approved permissions which are regularly and independently reviewed and updated.	Information only accessible to a small number of people that have approved permissions which are regularly and independently reviewed and updated.
Permission type	None required	Individual and group permissions suitable	Individual and group permissions are suitable. Least privilege best practice should be followed	Individual access should be granted, group permissions should be avoided where possible. Least privilege best practice must be followed
Impact if the information is breached	None	Minor financial and/or reputational damage to the University which may result in the reporting of a minor data privacy breach.	Moderate reputational and/or financial damage to the University which may result in the reporting of a moderate data privacy breach.	Significant financial and/or reputational damage to the University which may result in the reporting of a significant data privacy breach

Types of Information - See Information Handling guidelines for further examples	Publicly available Information which may include but not limited to; ● Campus Information ● Published course Information and timetables ● Marketing materials ● News Items ● Public Events ● Publications/Published papers ● Emergency or published University contact details	Internal Information may include but not limited to: ● Approved targeted Internal Communications ● Policies/Procedures/Standards/Guidelines ● Supplier Information ● University contact Information for staff not including Personally identifiable information (PII)	Restricted Information may include but not limited to: ● Contract Information ● Course materials including digital media and hard copies ● Non-Disclosure agreements ● Payslips/Pension information ● Staff and Student Personally identifiable information (PII) not including special category and health related details ● Usernames/LoginID	Highly Restricted Information may include but not limited to: ● Exam papers ● Financial, HR and legal information ● Passwords ● Staff and Student special category and health related details ● Research data ● Security information both physical and technical

Deciding what Classification to use

When deciding how to classify information it is important to consider the following:-

- The direct and indirect value of the information itself (the type of information). The nature of the information is at the heart of determining the classification.
- The risk of inappropriate disclosure, loss or loss of access to the information (the likelihood).
- The related costs to the University of identified risks occurring (the impact).
- The expectations of stakeholders who might have the authority to impose requirements i.e. legislative and regulatory requirements
- The need to control the extent of access to the information throughout its lifecycle
- The expectations of other organisations with whom the information is shared

Taking into account the above, considering in particular the content of the information, it should be possible to apply an appropriate Classification to the information being handled.

Originators of information or those responsible for information assets or systems are responsible for determining the Classification to be used. Guidance can be sought from colleagues in Information Security or Records Management to assist with this.

Documenting Classification decisions

A Classification can be applied to a particular information asset, or document type, a series of records, a specific report, or an information system. For particular information assets it should be possible to record the Classification within the Department's Information Asset Register. For more specific information assets such as a report, document, it is suggested that a physical indicator or marker be applied to highlight the classification. These markers should be placed in the header and footer of the document, and reflect the exact wording of the Classification Scheme. This is particularly relevant for papers marked Restricted or

Highly Restricted. If preparing a report or paper for a University Committee the appropriate marker should be placed on the cover page or executive summary sheet for the report before it is sent to the relevant committee.

Handling of Each Classification

The following section outlines how each classification should be handled and processed differently from the rest:

Handling Public Information:

Public information may be shared with third parties, on social media and in the public domain.

There are no extra precautions you need to take with handling and processing this class of information.

No special arrangements need to be made for secure storage or disposal.

There will still need to be arrangements in place to ensure that draft public information is appropriately approved and signed off.

It is good practice to mark this information as ‘Public’ when drafting, but remember to remove it when it is released as a public document into the public domain. No other specialist marking needs to be attached.

Care should be taken to ensure that the information you are handling is actually Public.

Examples of Public information includes:

- University social media posts
- Public facing University website content
- Marketing material
- Adverts
- Press releases

Handling Internal Information:

Internal information can only be accessed with a valid University account.

Care should be taken when needing to share this kind of information with anyone outside the University. This external sharing should be confirmed with your line manager.

It is good practice to mark this information as ‘Internal’ when drafting. No other specialist marking needs to be attached.

Examples of Internal information includes:

- University process, procedures and policies
- Non-public University website content (i.e. content that needs a University account to access)
- Handbooks
- Newsletters
- Directories
- Meeting agendas
- Information intended for future publication

Handling Restricted Information:

Restricted information should only be accessible to authorised users. Requests to access this kind of data requires sponsorship from your Head of Department, or designate.

Care should be taken when needing to share this kind of information with anyone inside and outside the University. This information should only be shared with those who need it to perform their role in or with the University. Sharing requires sponsorship and approval.

Please ensure appropriate access controls are in place at all times.

It is good practice to mark this information as ‘Restricted’ when drafting. No other specialist marking needs to be attached.

Examples of Restricted information includes:

- Personally identifiable information, not including Special Category data
- Specific or granular financial information such as financial forecasting information, granular breakdowns of costing or pricing information
- Documents, reports, papers containing an expectation of confidence information from external organisations, for example correspondence with Health professionals, Solicitors, or Procurement tenders
- Documents, reports or papers containing information used for future planning purposes
- Research data
- Information intended for future publication
- Information that would be exempt from provision under qualified exemptions within the Freedom of Information Act, for example correspondence relating to commercial interests, investigations and prejudice to law enforcement, health & safety.

Handling Highly Restricted Information:

Restricted information should only be accessible to a select group of authorised users. Requests to access this kind of data requires sponsorship from your Head of Department, or designate.

This information should only be shared with others in the University and with external parties when that sharing has been formally sponsored and approved and is performed in a secure way. This information should only be shared with those who need it to perform their role in or with the University.

Please ensure appropriate access controls are in place at all times.

It is good practice to mark this information as ‘Highly Restricted’ when drafting. No other specialist marking needs to be attached.

Examples of Highly Restricted Information

- Special Category Personal data
- Certain Research data
- Detailed financial information, the release of which would provide competitor institutions with information that could be used to the significant detriment or harm of the University
- Information received from external agencies such as the Police, Security Services or other organisations where there is a statutory or regulatory requirement to limit access.
- Information that would compromise the University’s ability to secure assets such as buildings, IT Services, information assets
- Information that would compromise the Health & Safety of University staff, students and stakeholders
- Information that would be exempt from provision under specific exemptions within the Freedom of Information Act
- Information that would prejudice the effective conduct of public affairs under Section 36 of the Freedom of Information Act.
- Information where there are absolute exemptions under the Freedom of Information Act for example personal data, or where there is a statutory bar on disclosure

Help & Further Information

If you’re unsure about the classification of the data you are handling, or how you should be handling a particular piece of information please get in touch with Matthew Zawadzki, the University Records Manager in the first instance - m.zawadzki@sheffield.ac.uk