



INFORMATION CLASSIFICATION POLICY

Policy owner:	University Secretary
Approver (Date):	UEB – 9 December 2025
Review due date:	Dec 2027
Current Version and update history:	1.0
Document Type:	Strategic Policy
Classification:	Public

Information Classification Policy

- 1. Introduction 3
- 2. Scope of Policy 3
- 3. Responsibilities 3
- 4. Definitions 3
- 5. Classification Categories 3
- 6. Handling requirements..... 4
- 7. Compliance and Monitoring 5
- 8. Related Policies 5

1. Introduction

- 1.1 The University creates and holds a wide variety of data and records which must be appropriately handled. This Policy establishes the framework for classifying and handling information at the University.
- 1.2 The Policy sets out the University's approach to identifying different categories of information according to the risks associated with loss, unauthorised disclosure, or misuse. It also specifies the appropriate controls required for the storage, transmission, sharing, and disposal of information.

2. Scope of Policy

- 2.1 This Policy applies to all University staff, students, contractors and partners who create, access, store, manage, or dispose of University information. It applies to both digital and physical records held by the University.

3. Responsibilities

- **University Executive Board:** Provide oversight, monitor compliance and ensure appropriate governance structures are in place to safeguard University information.
- **Audit Committee:** Review risk assessments relating to information security.
- **All Users:** Ensure information within their remit is correctly classified, managed, and protected in accordance with this Policy.

4. Definitions

- **Data:** any and all data recorded by the University, in any format.
- **Information Classification:** The process of assigning a level of sensitivity to information to ensure appropriate protection.
- **Personal Data:** Information relating to an identified or identifiable individual.
- **Processing:** Any activity involving the use, storage, modification, or transmission of information.

5. Classification Categories

- 5.1 All University data should be classified in line with the following four information classification levels:
 - Public** – Information intended for unrestricted public access with no anticipated harm arising from disclosure.
 - Internal Use** – Information for use within the University community where unauthorised disclosure could cause minor inconvenience or reputational impact.

Restricted – Information where unauthorised disclosure may result in significant harm, including legal, financial, operational, or reputational damage.

Confidential – Information requiring enhanced controls due to the substantial harm that may result from unauthorised disclosure, including serious legal or regulatory consequences.

6. Handling requirements

	Public	Internal Use	Restricted	Confidential
Examples	Published reports, prospectuses, marketing materials, website content, FOI responses, data of no commercial value or sensitivity	Internal memos, teaching materials not yet published, non-sensitive administrative data	Personal data, financial records not disclosed in annual reports, draft reports, sensitive meeting minutes, contracts, commercially sensitive information	Special category data, sensitive HR records, legally privileged information, restricted research data, financial details, trade secrets
Document marking	None	Internal	Restricted	Confidential
Storage requirements	May be stored on University systems or public platforms (ie university website)	Information must be held on University-managed systems, not on public platforms	Information should only be held on approved secure systems, eg access-controlled Sharepoint sites. Paper records must be stored in locked cabinets.	Information should only be held in encrypted format on approved secure systems. Paper records must be stored in locked cabinets.
Transmission and sharing	May be freely shared	May be shared on internal email and approved collaboration tools; avoid public dissemination	Encrypted email, secure file transfer, access-controlled Sharepoint areas	Only via University-approved encrypted transfer methods; strictly limited recipients
Disposal	Routine disposal via recycling or standard deletion - no restrictions	Secure deletion or confidential waste if printed	Secure deletion or confidential waste if printed	Secure deletion or confidential waste if printed

7. Compliance and Monitoring

7.1 The University will undertake regular reviews, audits, and monitoring activities to ensure compliance with this Policy. Non-compliance may result in disciplinary action and could pose risks under data protection legislation.

8. Related Policies

- Data Protection Policy
- Records Management Policy
- IT Acceptable Use Policy