DATA CLASSIFICATION AND HANDLING POLICY

1. INTRODUCTION

This Policy details how information should be categorised based on risk and sets out the required protective measures that must be used when handling different types of information.

1.1 Purpose

This Policy together with the Records Management Policy is intended to help members of the University determine the level of sensitivity of information, the appropriate handling methods and storage of information and what information can be disclosed to external parties.

1.2 Scope

This Policy:

- Is binding on all those who create or use University records such as staff, students, contractors, consultants, visitors and guests of the University, whether accessing records from on or off-campus;
- Applies to all records in electronic or hard copy format that are created, received and maintained by University staff in the course of carrying out their role;
- Includes records created, received and maintained in the course of research, whether internally or externally funded, in addition to any contractual and academic record-keeping requirements;
- Applies in all parts of the organisation including any records held by institutions partnered with the University;
- Applies when information is held by others on behalf of the University; for example where a Data Processor processes information on the instruction of the University, such as a contracted parking management company.

When information is held by the University solely on behalf of another person, for example where the University is acting as a Data Processor for research data under the instruction of another Institution, it is excluded from the scope of this policy.

2. POLICY

The classification of data is based on the level of sensitivity and the impact on the University should such data be disclosed, altered, lost or destroyed without authorisation. The classification of all data into different categories ensures that individuals who have a legitimate reason to access a piece of information can do so, whilst at the same time ensuring that data is protected from those who have no right to access the information. The classification will guide the appropriate security and technical controls required to be in place.

All data owned, used, created or maintained in any format within the University or on its behalf should be classified into one of four categories based on a risk assessment of its sensitivity or value, by those who own or are responsible for the information, or handle the information.

STEP ONE: Classification		STEP TWO: Handling	
Classification	**Description and Associated Risk**	**Handling and Storage**	**Disposal**
Open	Information that does not require protection and is considered “open and unclassified” and may be seen by anyone whether directly linked with the University or not. The information can be disclosed or disseminated without any restriction on content, audience, time of publication and would not breach any relevant laws or a duty of confidence.	No restrictions	No restrictions. Retain and destroy in line with the retention periods specified within the University Records Retention Schedule
Standard	Information intended for use inside the University that would only be made available to a person once they became a student, a member of staff or trusted external partner of the University. This could include some forms of personal data e.g. lists of students/staff. Information can be disclosed and shared with relevant individuals with minimal restrictions e.g. those who need access to the information to carry out their roles. The information would not be released into the public domain without some form of scrutiny to ensure that release would not cause any harm to individuals or the University. Any accidental or unauthorised disclosure would result in minor reputational damage to the University or individuals.	Information should be stored and shared on University approved systems. Paper records should be stored in secure / locked drawers / cupboards when not in use. If it is necessary to store information on portable media, it must be stored on encrypted media and removed once its purpose has been served. Information can be shared for business purposes, maintaining a need-to-know approach. The use of encryption or password protection should be considered but is not mandated. Extra consideration should be given to encryption if data is being transferred in large quantities. Physical assets should be protected in transit, not left unattended, and stored securely. Precautions should be taken to prevent overlooking or inadvertent access when working remotely or in public places. Post can be sent in the standard mail, but for large data sets Royal Mail ‘Signed For’ should be considered.	Information that is not freely available in the public domain should be destroyed in a way that makes reconstitution unlikely. Retain and destroy in line with the retention periods specified within the University’s Records Retention Schedule.
Confidential	Information that, if subject to unauthorised disclosure, dissemination or loss, could result in: a) A breach of a person’s privacy, which more likely than not would cause a moderate level of harm and/or inconvenience. This can also include opinions formed by the University on an individual and the University’s intentions towards an individual. b) Disruption to day-to-day operations of the University, where disruption only affects a sub-set of one particular area of the University. c) Damage to commercial relationships. d) Loss of competitive advantage.	Information must be stored and shared on University approved systems. Paper records should be stored in secure / locked drawers / cupboards when not in use. Where downloaded, data should be retained on University drives (personal or shared). Temporary downloaded data can be stored on encrypted password protected devices and deleted from any device at the end of each day. Data should only be held on One Drive, SharePoint or a Keele network drive that requires VPN access. Data can be shared via OneDrive or SharePoint or shared University drive as long as access is appropriately restricted. Data should not be communicated externally except in defined circumstances e.g. pre-agreed data sharing, police investigation. Sharing Confidential documents by email should be avoided where possible especially if this can be shared via OneDrive / SharePoint or other sharing method with appropriate access restrictions. If this is not possible, particular care should be taken to ensure emails are only sent to named recipients at known addresses and authorised staff should email using password protected attachments or use another encrypted transfer mechanism Where discussion in an open space or by telephone takes place, appropriate discretion should be exercised. Details of Confidential material should be kept to a minimum. Removal of physical assets should be confirmed with the asset owner. Physical assets should be protected in transit, not left unattended, and stored securely. Precautions should be taken to prevent overlooking or inadvertent access when working remotely or in public places. Post should be sent using Royal Mail ‘Signed For’ or equivalent.	Information should be destroyed in a way that makes reconstitution impossible. For example, paper files should be shredded and/or disposed of through Confidential Waste; all electronic devices should be wiped by IDS. Retain and destroy in line with the retention periods specified within the University’s Records Retention Schedule.
Highly Confidential	Information which is highly sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo.	Information must be stored and shared on University approved systems. Paper records must be stored in secure / locked drawers / cupboards when not in use. Where downloaded, data must be retained on University drives (personal or shared). Temporary downloaded data can be stored on encrypted	Information must be destroyed in a way that makes reconstitution impossible.

	Unauthorised disclosure, dissemination or loss could result in: a) Significant breach of a person's privacy, which more likely than not would cause substantial harm. b) Substantial risk to the health, safety and wellbeingof individuals or groups. c) Significant disruption to the University's operations . d) Irreparable damage to commercial relationships. e) The University being exposed to significant legal and / or financial risk. f) Significant reputational damage to the University or individuals.	password protected devices and deleted from any device at the end of each day. Data must only be held on One Drive, SharePoint or a Keele network drive that requires VPN access. Vital records, which are those vital to the continued functioning of the University in the event of a disaster, must be stored only on central Keele-based physical servers; e.g. current financial information, legal documents, research data and core student data. Data can be shared via OneDrive or SharePoint or shared University drive as long as access is appropriately restricted. Data must not be communicated externally except in defined circumstances e.g. pre-agreed data sharing, police investigation. Sharing Highly Confidential documents by email should be avoided where possible especially if this can be shared via OneDrive / SharePoint or other sharing method with appropriate access restrictions. If this is not possible, particular care must be taken to ensure emails are only sent to named recipients at known addresses and authorised staff must email using password protected attachments or use another encrypted transfer mechanism Highly Confidential data must not be discussed in public; if discussing via telephone, appropriate discretion must be exercised. Removal of physical assets must be confirmed with the asset owner. Physical assets must be protected in transit, not left unattended, and stored securely. Precautions must be taken to prevent overlooking or inadvertent access when working remotely or in public places. Post must be sent using Royal Mail 'Signed For' or equivalent.	For example, paper files should be shredded and disposed of through Confidential Waste; electronic devices must be wiped by IDS. Retain and destroy in line with the retention periods specified within the University Records Retention Schedule

For clarification or further advice, please contact the Joint Information Governance team comprising of Legal and Information Compliance and Information Security.

3. ROLES AND RESPONSIBILITIES

All information users are responsible for handing data in accordance with their classification and complying with this Policy and relevant legislation.

All data held by the University is classed as an information asset, as set out within the University's Information Governance Framework, and therefore must be included in the Information Asset Register held by each Directorate/Faculty/School. The Information Asset Register is the responsibility of each area's Information Asset Owner (IAO), who will be supported by Information Asset Managers (IAM) and, where necessary, Information Governance Champions to ensure that it is reviewed and updated regularly.

Information Asset Owners are responsible for ensuring the appropriate classification and handling of information within their respective areas and for putting in place appropriate processes to reflect the potential impact from compromise or loss. They are also responsible for considering any privacy issues when implementing new projects, processes or systems which involve the processing of personal data. Information Asset Owners should ensure that project leads undertake a Data Protection Impact Assessment (DPIA) as early as possible to identify the privacy risks and to put in place plans to mitigate those risks.

Where the University holds information on behalf of another organisation with its own classification system, an agreement must be reached to determine which set of classification and handling guidelines shall apply.

4. RELEVANT LEGISLATION

The University is subject to the provisions of the:

- GDPR / UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Reuse of Public Sector Information Regulations 2015

This is not an exhaustive list of legislation affecting Records management within the University as different business functions and activities are also subject to specific legislation or regulations, or to professional best practice or relevant ethical guidelines, for example, employment law, health and safety legislation and financial legislation.

The University will, so far as is practicable, seek to comply with relevant external documentation, such as guidance material from The National Archives, codes of practice, and other guidance material from the Information Commissioner. It will co-operate with other higher education institutions and other relevant public authorities with the aim of benefiting from best practice experience.

5. RELATED POLICIES AND PROCEDURES

This Policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- Data Protection Policy.
- Information Security Policy.

- Freedom of Information Policy
- Records Retention Schedule
- Clear Desk and Screen Policy
- Information Governance Framework
- Records Management and Handling Procedure (flowchart and examples)

6. REVIEW, APPROVAL & PUBLICATION

6.1 Review This Policy will be reviewed and agreed by the University Executive Committee before final approval.

6.2 Final Approval This Policy will require final approval from Council.

6.3 Publication This Policy will be published on the website within the Policy Zone. The University's Information Governance web pages will maintain prominent links to this Policy as appropriate on both external and internal facing pages.

9. DOCUMENT CONTROL INFORMATION

Document Name	Data Classification & Handling Policy
Owner	Director of Legal, Governance & Compliance
Version Number	V1.3
Equality Analysis Form Submission Date	NA
Approval Date	16/9/2021
Approved By	Council
Date of Commencement	16/9/2021
Date of Last Review	N/A
Date for Next Review	16/9/2024
Related University Policy Documents	Data Protection Policy Records Management Policy Records Retention Schedule Information Security Policy Freedom of Information Policy Information Governance Framework
Administrative update	10/03/2022: Head of Legal, Governance & Compliance updated to Director of Legal, Governance & Compliance
For Office Use – Keywords for search function	