Data Classification and Handling Policy

Classification:	Policy
Version number:	0-04
Status:	Approved
Approved by:	Information Governance Committee
Approval date:	4 August 2022
Effective from:	5 August 2022
Next review date:	4 August 2025
Document author:	Data Protection Manager
Document owner:	University Secretary, Registrar and Chief Compliance Officer
Contact:	University Secretary Office
Collaborative provision:	Mandatory

State whether this document is applicable to the University's collaborative partners

Related documents:	Data Protection Policy; Data Breach Policy
University document:	No

A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.

Published location:	Website

· All printed or downloaded versions of this document are classified as uncontrolled

Data Classification and Handling Policy

Table of Contents

Version 0-04 of this document was approved by Information Governance Committee on 04 August 2022

Data Classification and Handling Policy

1 Introduction

1.1 The University generates and holds a wide variety of data and like any other business asset that data must be protected appropriately against unauthorised access, disclosure or misuse.

2 Scope

2.1 This policy applies to all University Staff, Students, Contractors and volunteers working for the University.

3 Purpose

3.1 The purpose of this Policy is to set out the protections that should be applied to the different types of data that are handled within the University. Applying a set of principles consistently throughout the University will assist to ensure that data is processed securely, thereby preventing security breaches and minimizing the impact of any breaches that do occur.

3.2 Compliance with this Policy will help the University to meet the University Information security requirements that the appropriate degree of protection is applied to all data, the security requirements within General Data Protection Regulation (GDPR) in respect of personal data, reduce risk and assist in the efficiency when processing Freedom of Information requests.

4 Definitions

4.1 The definition of data used by this policy is 'any and all data recorded in any format by the University'. This includes paper notes, documents, electronic files, video and audio recordings.

5 Responsibilities

A Information Governance Committee

5.1 The Information Governance Committee is responsible for:

a. Approving the Information classification markings and associated data management policies.

b. Promoting and publicising the classification policy and the importance of its use.

B Data Owners/Stewards

5.2 The Data Owner may delegate responsibilities, but will retain accountability.

5.3 The Data Owner is required to:

a. Ensure the appropriate classification is assigned

b. Manage and authorise appropriate access to the data

c. Identify additional controls required to ensure the confidentiality, integrity and availability of the data.

d. Communicate the handling requirements to users of the data.

e. Consider the potential risks and develop a business continuity plan.

C All members of the University staff, students including contractors.

5.4 It is the responsibility of the individual handling data to be aware of this policy and apply the protections appropriate to the class of data, especially where not marked.

5.5 All are responsible for handling of data in compliance with this Policy.

6 Categories of data

6.1 Data and assets shall be classified in terms of their value, legal requirement, sensitivity and criticality to the University.

6.2 When considering classification consider:

a. Confidentiality – What impact would the unauthorised disclosure of the data have?

b. Integrity- What impact would there be if the data was modified or deleted?

c. Availability – What would the impact be if the data was not available for a period of time?

6.3 All University data should be classified into one of the following four levels:

A Confidential

6.4 Confidential Data carries significant value to the University and any unauthorised disclosure or sharing of that data could lead to severe reputational damage and financial penalty.

6.5 Therefore, limited to only those that have 'Need to Know' and are explicitly granted access.

B Restricted

6.6 Restricted Data where the disclosure or sharing of the data to the public would not be expected and may incur reputational and financial damage.

6.7 Therefore. it is open to those with specific requirement to view subject to controls in place.

C Internal Use

6.8 Data intended for and available for internal use only. Data of limited value and sensitivity however may impact individuals as the expectation that it would not be made available to the wider public.

D Public

6.9 This data is suitable for release or accessible to the general public with no restrictions.

7 Data protection

7.1 The Data Protection Act 2018 and General Data Protection Regulation set out the obligations that apply to the University when handling Personal Data.

7.2 Those handling Personal data must follow the University's Policies & Procedures in respect of Data Protection https://www.hull.ac.uk/policies.

8 Freedom of Information

8.1 The Freedom of information Act 2000 requires the University to consider any request for any information from any individual anywhere in the world, The presumption is on disclosure.

8.2 As such, each request for information must be assessed according the particular circumstances of the data requested. The data classification applied will not act as an automatic bar to disclosure, however the reasons for applying the classification will be taken into account and may serve to support any evidence of harm and/or public interest when considering exemptions.

8.3 The University will follow the University Freedom of Information Policy for all data captured by the terms of a request.

9 Version control

Version	Author	Date approved	Relevant sections

10 Appendix A: Data classification

	Public	Internal	Restricted	Confidential
Personal data	No Personal Data, or disclosure of Personal Data would be reasonably expected by the Subject.	Contains Personal Data, but disclosure would not normally be reasonably be expected by the Subject.	Contains Personal Data, but disclosure would not be reasonably be expected by the Subject and would cause some damage and distress	Contains Special Categories of Personal Data (Appendix B) and or other data which compromise would result in high impact to an individual
Examples	Personal Data made public on university websites, with consent	- Personal details held on Active directory - Attendees at meeting	- Employee records; - Student data; - databases and spreadsheets containing personal data; - Personal data within email messages	- Occupational Health records. - Email messages containing special categories of personal data. - Disciplinary proceedings; - Financial, bank details
Other data	**Data of no commercial value or sensitivity**	**Data of limited value or sensitivity**	**Data of serious value or sensitivity**	**Data of critical commercial value or sensitivity**
Examples	- Freedom of Information Responses - Information within the Publication Scheme (including Policies & Procedures) - Information published to the University website	- Policies exempt from disclosure under Freedom of Information Act 2000 - Information on Notice Boards - Internal memos	- Contracts - Reserved committee minutes - Financial information (not disclosed in Financial Statements - Technical or commercially sensitive info - Research proposals	- Trade secrets - Security Sensitive research material - Legally privileged information

11 Appendix B: Special category

11.1 Under the General Data Protection Regulations Special Categories of Personal Data are those revealing:

a. Racial or ethnic origin;

b. Commission or alleged commission of any offence; and,

c. Political opinions;

d. Religious or philosophical beliefs;

e. Trade union membership;

f. Genetic data, biometric data processed for the purpose of uniquely identifying a natural person;

g. Data concerning health; or,

h. Data concerning a natural person's sex life or sexual orientation.

i. And Under Article 10 Criminal conviction data

12 Appendix C: Data handling

	Public	Internal Use	Restricted	Confidential
Data Storage	Can be stored on any device and on the internet. No restrictions on printing and copying this data, subject to copyright restrictions.	Data must be held within systems provided or sanctioned by the University as listed in the Information Systems and Data governance Register. Paper documents must not be left unattended.	Data must be held within systems provided or sanctioned by the University as listed in the Information Systems and Data governance Register. Paper records should not be left unattended and must be stored in locked drawers or cabinets.	Data must be held within systems provided or sanctioned by the University as listed in the Information Systems and *Data governance Register*. Paper records should not be left unattended and must be stored in locked drawers or cabinets.
Data Access	No restriction	Appropriate controls should limit access to only those members of the University that require it.	Data should only be placed in areas with restricted access. Data held within information systems must be controlled as described in the *User Management Policy*.	Data should only be placed in areas with restricted access. Data held within information systems must be strictly controlled as described within University Policies. https://www.hull.ac.uk/policies

	Public	Internal Use	Restricted	Confidential
Data Transfer/Sharing	Data may be freely transmitted without restriction.	Data may be placed on the University SharePoint service and sent via internal email with appropriate controls on access. Data may be sent via internal email with appropriate care in addressing. Data should not generally be transferred to any non-ICTD managed mobile devices as described in the File Storage *Policy*.	Where possible, data within information systems should be access within that system and not exported or shared. If transfer or sharing is required then appropriate controls must be used to safeguard the data. Data should only be transferred to encrypted mobile devices. Encryption must be used when emailing data to external recipients unless prior agreement e.g. Personal Data requests. Items sent by internal and external mail should be placed in sealed envelopes.	Where possible, data within information systems should be access within that system and not exported or shared. If transfer or sharing is required then appropriate technology, such as encryption, must be used to safeguard the data. Data should only be transferred to encrypted mobile devices. Hard copies of documents should be hand delivered internally. External mail should be special delivery signed for and double enveloped.
Document Marking	None.	'INTERNAL USE ONLY' on document coversheet (if applicable) and on each page.	'RESTRICTED' on document coversheet (if applicable) and on each page.	'CONFIDENTIAL' on document coversheet (if applicable) and on each page.
Disposal	No restrictions.	Paper documents must be crosscut shredded. Electronic media must be securely wiped.	Paper document must be crosscut shredded. Electronic media must be securely wiped.	Paper document must be crosscut shredded. Electronic media must be securely wiped.