UNIVERSITY OF HULL

Data Classification and Handling Policy

Approved by: Information Governance Committee
With effect from: August 2018 **Next date for review: August 2019**
Other related policies: To be read in conjunction with the Data Protection Policy
Contact for further information: Information Compliance Officer (infocompliance@hull.ac.uk)
Reference to any superseded policy/amalgamations:.
Classification: Public
Relevant legal framework: Data Protection Act 2018
Equality analysis: The implementation of this policy is not considered to have a negative impact on protected characteristics.
Freedom of information: This Guidance is publicly available through the University's Publication Scheme under the Freedom of Information Act 2000.

Version	Changes
0.1	First Draft

1. Purpose

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 mean that data is processed securely, thereby preventing security breaches and minimizing the impact of any breaches that do occur.

Compliance with this Policy will help the University meet the requirements of the General Data Protection Regulation (GDPR), reduce the time spend handling Freedom of Information requests and help to prevent 'phishing' breaches.

2. Scope

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

This policy applies to all University Staff, Students, Contractors and volunteers working for the University. Individuals are responsible for assessing the information they work with and applying the appropriate classification, and hence controls.

3. Responsibilities

Responsibility for applying the correct classification lies with the information owner. For example, this could be the document author or Information System Owner (as set out in the Data Protection Policy).

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.

4. Categories of data

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

- **Confidential** – Access limited to a select group of individuals (high risk).
- **Restricted** – Access limited to those with a requirement to view (medium risk).
- **Internal use** – Access generally limited to Staff and Students of the University (low risk).
- **Public** - may be viewed by any member of the public (no risk).

4.1. Applying a classification

Data will be classified according to the impact on the University in the following areas (as set out in the Information Governance and Assurance Policy):

- **Confidentiality** – what impact would unauthorised disclosure of the data have?
- **Integrity** – what impact would modification or deletion of the data have?

- **Availability** – what impact would disruption to access to the information have on the University?

Information should be classified according to the table at Appendix A. Data may not sit clearly within any one of the below classifications, and so the individual applying the classification or handling the data should apply the higher classification to the whole document.

5. Data Handling

Once classified, data must be handled according the table at Appendix C.

6. Data Protection

The Data Protection Act 1998 and General Data Protection Regulation set out the obligations that apply to organisations such as the University when they handle Personal Information.

Those handling personal data must follow the University's Policies and Procedures in respect of Data Protection, such as:

Removable Media Policy
User Management Policy

7. Freedom of Information

The Freedom of Information Act 2000 requires the University to consider any request for any information from any individual from anywhere in the world. Disclosure of information is the default.

As such, each request for information must be assessed according the particular circumstances of the data requested. The data classification applied will act as 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 the application of an exemption.

The University will follow the same process as set out in the University's Freedom of Information Code of Practice for all data captured by the terms of a request.

Appendix A – Classification Matrix

	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.	Contains Special Categories of Personal Data (Appendix B).
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	○ Press Releases; ○ Freedom of Information Responses; ○ Information within the Publication Scheme (including Policies & Procedures); and, ○ Information published to the University website.	○ Policies exempt from disclosure under Freedom of Information Act 2000; ○ Information on Notice Boards; and, ○ Internal memos.	○ Employee records; ○ Student data; ○ Contracts; ○ Reserved committee minutes; ○ Financial information (not disclosed in Financial Statements); and, ○ databases and spreadsheets containing personal data; ○ Personal data within email messages.	○ Passwords; ○ Security Sensitive research material; ○ Disciplinary proceedings; ○ Legally privileged information; and ○ Occupational Health records. ○ Email messages containing special categories of personal data.

Appendix B –Special Categories of Personal Data

Under the General Data Protection Regulation **Special Categories of Personal Data** are those revealing:

- Racial or ethnic origin;
- Commission or alleged commission of any offence; and,
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data, biometric data processed for the purpose of uniquely identifying a natural person;
- Data concerning health; or,
- Data concerning a natural person's sex life or sexual orientation.

Appendix C –Data Handling Matrix

	Classification			
	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.	Information must be held within systems provided or sanctioned by the University as listed in the *Data governance for information systems* document. Paper documents must not be left unattended.	Information must be held within systems provided or sanctioned by the University as listed in the *Data governance for information systems* document. Paper records should not be left unattended and must be stored in locked drawers or cabinets.	Information must be held within systems provided or sanctioned by the University as listed in the *Data governance for information systems* document. 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 the *User Management Policy.*
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 *Removable Media 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. 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 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.