UNIVERSITY OF HULL

Data Protection Policy

Classification:	**Policy**
Version Number:	6-0
Status:	Approved
Approved by:	University Leadership Team
Approval Date:	06/02/2024
Effective from:	06/02/2024
Next Review Date:	06/02/2026
Document Author:	Angela Clement, Data Protection Officer
Document Owner:	Chris Ince, University Secretary & Chief Compliance Officer
Department/Contact:	Governance & Compliance dataprotection@hull.ac.uk
Collaborative provision:	State whether this document is applicable to the University's collaborative partners: ☒ Mandatory ☐ Not mandatory
Related documents:	Information Governance Assurance Policy, Data Breach Policy, Data Protection Privacy Impact Assessment Policy, University COP for Research Misconduct
University Document?:	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. **Yes**
Published location:	Website/SharePoint
The University has adopted the principles of **Designing For Diverse Learners**, and all policy documents should be written with reference to these principles. Further information is available at Designing for diverse learners.info.	
An Equality Impact Assessment must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.	

This document is available in alternative formats from

policy@hull.ac.uk

UNIVERSITY OF HULL

Data Protection Policy

Table of Contents

UNIVERSITY OF HULL

Data Protection Policy

1. Introduction

1.1 The University of Hull treats very seriously both the personal data and sensitive personal data it processes on behalf of students and staff members and the wide range of other people with whom it has contact.

1.2. This policy provides a framework for ensuring that the University meets its obligations under the General Data Protection Regulation (GDPR) and associated legislation enacted in the UK e.g. Privacy and Electronic Communications (EC Directive) Regulations 2003.

This policy is to enable the University of Hull to:

- Ensure compliance with GDPR, Data Protection Act 2018 and associated legislation.
- Ensure all staff are aware of their statutory duties and responsibilities under the legislation
- Demonstrate its commitment to privacy, confidentiality and the proper handling of personal data;
- Protect the organisation from the consequences of any breach of its statutory and common law responsibilities; and,
- To provide clarity to staff and ensure all are aware that failure to comply or any deliberate beach of this policy will result in disciplinary action.

2. Scope

This Policy applies to all personnel handling personal data University Staff, Students, and volunteers working for the University. It also applies to 3rd party suppliers/contractors if by virtue of their role they, are required to access or handle personal data of the University

3. Definitions

Personal Data – Information relating to a living and identifiable individual. It also extends to any expression or opinion about an individual and any intention of the Controller towards the individual;

Data Subject – A living and identifiable individual who is the subject of personal data;

Consent – freely given, specific informed and unambiguous indication of the data subjects wishes;

Controller – An organization that has control of and determines the processing personal data and/or sensitive personal data;

Processor – Any person or organization other than the controller (or an employee of the data controller) who processes the data on behalf of the data controller;

Process – to obtain, store, hold, disclose, anything that we do with personal data from the point of collection to destruction;

Sensitive Personal Data – also known as **special category data and criminal offence data**. Sensitive personal data that falls into one of the categories below:

- Sexual life;
- Race;
- Religion;
- Political opinions;
- Trade union membership;
- Physical and mental health;
- Commission or alleged commission of any offence; and,
- Proceedings, disposals and sentence in relation to the commission or alleged commission of any offence.

Third Party – Any person or organization other than the data subject, data controller or data processor.

4. Associated Documents & Guidance

4.1. The University also publishes Data Protection related policies and guidelines, which includes guidance and advice for staff on the following areas:

Collecting and processing personal data: Appropriate Policy Doc; Data Protection Privacy impact assessment Policy and guidance, Data Processing Contract template and checklist;

Disclosing personal data: Subject access Rights Procedure and Data Sharing Policy and template;

The retention and disposal of personal data: Retention Schedule & File Storage Policy

Keeping personal data secure: Data Classification and Handling Policy including emailing personal data safely, providing personal data safely over the phone, sending personal data in the post, using paper records out of the office; Information System Assurance Policy defines roles for System Owners to safeguard personal and sensitive data

Managing information security breaches: Data Breach Policy

5. Areas of Responsibility

The Data Protection Act 2018 (DPA) and GDPR applies to all staff, students, contractors and volunteers working for the University. The University is a Controller, as defined in Section 1 of the DPA, and is obliged to ensure that the DPA's requirements are implemented, monitored and evaluated.

5.1 University Leadership Team

The University of Hull Leadership Team have overall responsibility for ensuring that the organisation complies with its legal obligations.

5.2 University Senior Information Risk Owner (SIRO)

The University Secretary and Chief Compliance Officer is the University Senior Information Risk Owner and takes responsibility for operating a framework for assessing risks to information across the organisation, for investigating incidents involving breaches or potential breaches of information security and approving unusual or controversial disclosures of personal data to other organizations.

5.3 Information Governance Committee

The primary function of the Information Governance Committee (IGC) is to oversee, and provide leadership in, efficient and effective information management within the University. Oversight of information management shall include oversight of:

- Information Assurance;
- Data Quality management;
- Information and data ownership;
- Information Management policy;
- Information risk management;
- Information breach management;
- Recommendations as to required training.
- Data Sharing

IGC will act as primary decision making authority on data protection related matters, reviewing and approving data protection related policies and processes, acting as a point of escalation for compliance issues, ensuring level of resource to deliver approved strategies

and ensuring the DPO has appropriate levels of autonomy and adequate levels of resource in order to allow them to undertake their role effectively and fulfil the requirements of the role.

5.4 **Data Protection Officer**

The Data Protection Officer (DPO) is responsible for monitoring internal compliance with data protection legislation. Their responsibilities include:

- Briefing the IG Committee on their Data Protection responsibilities;
- Dealing with all correspondence between the University and the Information Commissioner's Office;
- Reviewing and updating Data Protection and related policies and obtaining approval by IGC and ULT;
- Providing specialist advice to staff on Data Protection issues; including data protection breaches;
- Manage and deal with subject access requests and bringing issues to the attention of the University Secretary;
- Update and maintain Article 30 Records of Processing Activity (RoPA).

5.5 **Communications**

The Head of Marketing and Communications is responsible for approving any statements on publicity materials or similar releases with an impact on Data Protection or privacy.

5.6 **Managers**

Staff line managers are responsible for ensuring this policy and its associated guidelines are understood and implemented by their staff. Managers will ensure that staff processing personal data receive Data Protection training.

5.7 **Staff**

All staff (at all levels of the University) who process personal data must read and comply with the University's Data Protection Policy, undertake mandatory training and refresher training every two years. Staff who process personal data will obtain, store, and use data in compliance with the DPA principles and in a confidential manner. All staff are responsible for reporting any breach or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of personal data.

5.9. **Students**

Students may, during the course of their studies/research, gather or process personal information about other identifiable, living individuals (e.g. through the use of interviews, questionnaires or primary sources). Students are expected to treat this personal data in a manner compatible with this Policy and its associated documents.

Students must ensure that any information they provide to the University is accurate and is kept up-to-date by notifying the University of any alterations to address, personal details or course enrolments.

5.8 **Volunteers and third parties**

Volunteers are expected to abide by this policy and its associated documents. Volunteers processing personal information will also be expected to undertake mandatory training.

Arrangements with third parties and data processors handling University owned personal data must follow the University's Data Protection Policy

6. The Principles

The GDPR sets out seven key principles that organisations most follow. The University expects all staff, students, volunteers and visitors handling personal data to abide by the Data Protection Principles outlined below:

Lawfulness, fairness & transparency

- Personal Data should be processed lawfully, fairly and in a transparent manner.
  For Data to be processed transparently, individuals must be given clear and adequate information before their data is collected so that they understand how and why their personal data will be used and are able to make informed decisions in respect of processing their data.
  For data to be processed lawfully one of the legal basis as set out in Data Protection Law must apply
    - Consent – Consent must be freely given, specific, informed and unambiguous.
    - Contract – Necessary for fulfilling a contract or to enter into a contract
    - Legal obligation – Necessary to comply with the law.
    - Public task – Necessary to perform a task in the public interest or for an official

function

- Legitimate Interests – Necessary for the University's legitimate interests or the legitimate interest of another party, unless it would undermine the interests of an individuals right to privacy.
- Vital Interests – Necessary to protect the life of the individual or another individual

There are additional safeguards when processing sensitive special category data see Appendix A.

Purpose Limitation

- Personal Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

Data Minimisation

- Personal Data processed should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); Where possible Personal data should be anonymised or pseudonymised at the earliest opportunity.

Accuracy

- Personal Data processed should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation

- Personal Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; When no longer needed for the purpose for which collected and if there is no lawful basis to continue to retain the persona must be either fully anonymised or deleted in accordance with University Retention Schedule.

Security

- Personal Data Should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The controller shall be responsible for, and be able to demonstrate compliance with Principle 1 accountability.

7. Training

In accordance with the University Mandatory Training Map, it is the policy of the University that every individual who *'…use(s) University IT systems, including email, that may contain personal data'* must complete the 'Data Protection and IT security' online learning module. This training must be completed at least once in every two-year period. Completion of additional, or alternative, training may be required for specific roles depending on an assessment of risk.

8. Subject Rights

8.1. Subject Access

The University of Hull acknowledges and respects that Data Subjects (whatever their relationship with the University) have the right to be informed about the collection and use of their personal data.

The right to be informed
The right of access to that data and receive copies of their Personal Data.

Individuals also have the additional rights:
The right to rectification. To have inaccurate personal data rectified or completed.
The right to erasure (or to be forgotten) to ask for personal data to be erased; this is not absolute, and will only occur in limited circumstances.

8.2. Direct Marketing

The University of Hull will comply with the requirements of the Privacy and Electronic Communications Regulations 2003 (PECR) in respect of direct marketing. As such, telephone calls to those registered with the Telephone Preference Service (TPS) and all electronic mail that falls under these Regulations will only be made where specific opt-in consent has been given. An option to opt-out of any form marketing will be offered in each instance of marketing, and any withdrawal of consent will be recorded and respected.

All telephone numbers will be screened against the Telephone Preference Service prior to a relevant marketing call being made.

A Privacy Notice will be provided to all individuals at the time this consent is recorded.

8.3. **Right to object**

The University acknowledges that a Data Subject has the right to object to any processing activity carried out the University that they consider causes them unwarranted and substantial damage and distress, unless:

- the Subject has consented to the processing;
- the processing is necessary:
- in relation to a contract that the Subject has entered into; or
- because the Subject has asked for something to be done so they can enter into a contract;
- the processing is necessary because of a legal obligation that applies to the University (other than a contractual obligation); or
- the processing is necessary to protect the Subject's "vital interests".

Any such objections should be addressed to the Data Protection Officer dataprotection@hull.ac.uk and must specify the reason why the processing has this effect.

8.4. **Right to have Personal Data Rectified, Blocked, Erased or Destroyed**

The University will comply with the fourth Principle, and will correct out of date or incorrect Personal Information if and when made aware of it.

9. Audit and Assurance

Privacy By Design - Data Protection Impact Assessment (DPIA)

The University will review all new projects, services and redesigned projects and services to consider whether it is likely to result in a high risk to the rights and freedoms of natural persons, and whether therefore a DPIA is required.

Data Protection Audit

The Data Protection Officer and ICT Manager / representative will conduct or commission regular compliance audits of Information Security and Data Protection training and major services and processes to ensure that the Data Protection Act and the security of our systems is complied with.

10. Sanctions

The University regards any breach of data privacy legislation, this policy or any other policy and or training introduced by the University to comply with data protection legislation as a serious matter.

Any breach of this policy may be considered under the Student Disciplinary Regulations or the Staff Disciplinary Policy and Procedure.

All those covered by this policy should be aware that there are also several criminal offences under section 170 of the Data Protection Act 2018 or Computer Misuse Act 1990, which an individual may be personally liable specifically those relating to:

- selling, obtaining and disclosing personal data knowingly or recklessly without the consent of the University, and retaining personal data without the consent of the Controller
- unauthorised access to, and/or modification of computer material.

Staff, students, visitors and volunteers must therefore not access or disclose personal information for any purpose outside of normal requirements of their role.

Any confirmed or suspected Data breaches should be reported promptly to the Data Protection Officer in line with the Data Breach Policy.

11. Review

The Data Protection Officer will be responsible for ensuring that this policy and its associated procedures are reviewed at least every two years.

Version Control

Version	Author	Date approved	Relevant sections
5-0	Angela Clement (Data Protection Officer)	09/11/2021	
6-0	Angela Clement (Data Protection Officer)	06/02/2024	4/5/6