UNIVERSITY OF HULL

Data Protection Policy

Classification:	Policy
Version Number:	4-0
Status:	Draft
Approved by:	University Leadership Team
Approval Date:	09/11/2021
Effective from:	09/11/2021
Next Review Date:	09/11/2023
Document Author:	Angela Clement, Data Protection Officer
Document Owner:	Chris Ince, Chief Compliance Officer
Department/Contact:	Governance & Compliance dataprotection@hull.ac.uk
Relevant Legal Framework	Data Protection Act 2018, EU & UK GDPR, Freedom of Information Act 2000, Human Rights Act 1998, Privacy and Electronic Communication Regulations 2003.
Related documents:	Information Governance Assurance Policy, Data Breach Policy, Data Protection Privacy Impact Assessment Policy, University COP for Research misconduct
Published location:	Website
Freedom of Information:	This policy is suitable for publication.

All printed or downloaded versions of this document are classified as uncontrolled.
A controlled version is available from the university website.

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. Under the Data Protection Act 2018 (DPA 2018) and the UK version of the General Data Protection Regulation (UK GDPR), The University is classed a Controller. The University is also required to comply with EU GDPR. The principles and rights of individuals contained within the EU GDPR are the same as the UK GDPR. For the purposes of the is Policy GDPR will apply to both EU GDPR and the UK GDPR

1.2. This policy is to enable the University of Hull to:

- Ensure compliance with GDPR and Data Protection Act 2018.
- 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:** Data Protection Privacy impact assessment Policy and guidance, Data Processing Contract template and checklist;

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

- The retention and disposal of personal data: Retention Schedule

- Keeping personal data secure: Data Classification and Handling Policy including emailing personal data safely, providing personal data safely over the phone, sending persona data in the post, using paper records out of the office;

- 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 organisations.

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;
- Manage and deal with Freedom of Information (FOI) requests bringing issues to the University Secretary;
- Update and maintain Article 30 Records of Processing Activity (RoPA).

5.5 **Core Information Systems**

The University has developed a register of core information systems and identified positions of responsibility (as below) that correspond to the area that operates each system. This table is maintained by the University's Information Governance Committee.

Executive Senior Information Risk Owners

Executive SIROs will assume responsibility for the University's core systems. They are accountable for the assurance of information security at the University, and appoint Information System Owners to safeguard personal and sensitive data. Information System Owners provide assurance to the Executive SIRO on an annual basis.

Information System Owners

Information System Owners will be appointed by the relevant Executive SIRO. Information System Owners are expected to:

- understand the purpose of information assets in their systems, how they are held, accessed and removed;
- understand how information is shared and transferred within their systems and how access to the information is restricted;
- sign off compliance documents, including risk assessments, for information assets within their systems;
- escalate risks to information to their Executive SIRO as necessary.

Information System Steward

Information System Stewards will be appointed by the relevant Information System Owner.

Information System Stewards are expected to:

- understand the purpose of information assets in their systems and have the day to day responsibility for how they are held, accessed and removed;
- understand how information is shared and transferred within their systems and have the day to day responsibility for how access to the information is restricted;
- work with Data Protection and Information Security specialists to assess risks to information, and how those risks can be managed

5.6 **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.

5.7 **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.

5.8 **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.

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.

5.9 **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 University expects all staff, students, volunteers and visitors handling personal data to abide by the Data Protection Principles outlined below:

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- 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');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 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 ('accuracy');
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- 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 ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with P1 accountability.

6.1 **Obtaining**

Only personal data that is necessary for a specific University-related business reason should be obtained.

When obtaining personal data staff must first ensure that the purpose under which they are collecting the data is included in the University's notification. If it is not they should notify the Data Protection Officer before any personal data is collected so that the notification can be amended.

A privacy notice (also known as a fair processing notice or a data protection statement) must be actively communicated to individuals at the point at which their personal data is collected and ideally should be in the same medium. A privacy notice must as a minimum explain who you are, what you intend to do with the personal data and who it will be shared with or disclosed to. It is also good practice to include further information in a privacy notice, for example how long the data will be kept for, how the data will be kept secure, the consequences of not providing the data and the right to make a subject access request. Further guidance on writing privacy notices is available from the Data Protection Officer

In some cases individuals will have a choice over whether or not to provide their personal data, or over the use that can be made of it. In these cases clear consent must be obtained.

It is the policy of the University that the minimum amount of information necessary to achieve a business purpose will be processed (in accordance with Principle 1-3 of the DPA). Consideration should therefore be given to whether business objectives can be met without the processing of personal information at all through anonymisation, and secondly whether personal data can be pseudonymised.

6.2 **Recording**

Staff must ensure that mechanisms are put in place for keeping personal data accurate and up-to-date for the purpose for which it is held.

Personal data should be retained in accordance with the University of Hull's retention policy.

Staff should be aware that any material they produce that refers to individuals may be accessed by that individual regardless of the informality of that information or how or where it is held, including

any opinion of an individual. Staff should be aware of this when documents are created.

6.3 **Storing**

All staff whose work involves processing personal data, must take personal responsibility for its secure storage.

Access to personal data, in electronic or paper format, should be restricted to staff who need to access the information in the course of their duties.
Personal data in paper format must be kept in a locked filing cabinet, cupboard or drawer. Documents containing personal data should only be printed when there is a business need to do so. Documents should not be automatically (push) printed to shared print devices unless staff take other appropriate measures to ensure the security of the data.
Personal data in electronic format should be stored within the University Data Centre which is regularly backed up and should not be kept on local hard drives. As a minimum, user accounts should be password protected and consideration should be given to the use of additional folder, file or database level password protection, access restrictions and/or encryption. Staff can contact the University's ICT Service Desk for advice on how to do this.

Staff who intend to store personal data on a portable storage device, such as a laptop, tablet, memory stick, hard drive, disk or mobile phone, must seek the authorisation of their line manager. The personal data on the portable storage device must be encrypted and the device must be kept in a locked filing cabinet, cupboard or drawer.

Staff must not keep sensitive personal data on portable storage devices unless they have received authorisation from both their line manager and the Data Protection Officer.
Normally personal data should never be stored at staff members' homes, whether in paper or electronic format. In instances where off-site processing is necessary, staff must obtain authorisation from their line manager. If the processing includes sensitive personal data authorisation of their line manager and the Data Protection Officer is required

6.4 **Transferring**

Any transfer of personal data must be done securely and in line with the University's ICT Regulations and Guidelines.

Email is not a secure method of communication and sending personal data via external email should be avoided unless it is encrypted, with the password provided to the recipient by separate means such as via telephone.

While internal email (within the University's email system) is more secure, it is still advisable to consider encrypting attachments which contain data belonging to a large number of data subjects or sensitive personal data in order to mitigate the risks associated with emails being sent or forwarded to unintended recipients.

Emails containing personal data should be marked 'confidential', have an appropriate subject heading and explain clearly to the recipient why they are being sent the information and what they are expected to do with it.

Care should be taken to ensure that emails containing personal data are not sent to unintended recipients. It is important that emails are correctly addressed and that care is taken when using the reply all or forwarding functions or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple people to avoid disclosing personal information to other recipients, for example personal email addresses or other information that could be deduced simply by their inclusion in the email distribution.

Personal email accounts must not be used to send or receive personal data for work purposes.

When sending personal data externally, either in paper format or in electronic format on a portable device, a Royal Mail tracking service or a courier service must be used. If personal data is being sent via Royal Mail, it is recommended that the 'Special Delivery' service is used, particularly if sensitive personal data is being transferred.

Personal data stored on portable devices must also be encrypted. When sending personal data internally in paper format it should be sealed in an envelope marked confidential and ideally hand-delivered to the recipient. If personal data is sent via the University's internal mail the 'internal recorded' system should be used. This requires 'Internal Recorded' and the name of the sender to be written on the top right-hand corner of the envelope.

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 of access to that data request and receive copies of their Personal Data.
See Information Rights Policy.

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.

Data Subjects also have the right to apply to a court for an order to rectify, block, erase or destroy the inaccurate information.

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

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 several criminal offences under section 170 of the Data Protection Act 2018 or Computer Misuse Act 1990, 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.

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.