Data Protection Policy

February 2026

This policy explains how the University protects and manages personal data in compliance with the UK GDPR and the Data Protection Act 2018. It applies to all staff, students, volunteers and third parties, outlining responsibilities, principles, subject rights, training, audit requirements and consequences of non-compliance.

Contents

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 Data Protection Act 2018 (DPA 2018), the Data (Use and Access) Act 2025, the UK General Data Protection Regulations (UK GDPR) and associated legislation enacted in the UK, for example the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

1.3 This policy is to enable the University to

a. ensure compliance with the UK GDPR, the DPA 2018 and associated legislation

b. ensure all staff are aware of their statutory duties and responsibilities under the legislation

c. demonstrate its commitment to privacy, confidentiality and the proper handling of personal data

d. protect the organisation from the consequences of any breach of its statutory and common law responsibilities

e. 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

2.1 This policy applies to all personnel handling personal data: staff, students, and volunteers working for the University. It also applies to third-party suppliers/contractors if, by virtue of their role, they are required to access or handle personal data of the University.

3 Definitions

3.1 **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.

3.2 **Data subject:** a living and identifiable individual who is the subject of personal data.

3.3 **Consent:** freely given, specific informed and unambiguous indication of the data subjects wishes.

3.4 **Controller:** an organisation that has control of and determines the processing personal data and/or sensitive personal data.

3.5 **Processor:** any person or organisation other than the controller (or an employee of the data controller) who processes the data on behalf of the data controller.

3.6 **Process:** to obtain, store, hold, disclose, anything that we do with personal data from the point of collection to destruction.

3.7 **Sensitive personal data** (also known as **special category data** and **criminal offence**

data): Sensitive personal data that falls into one of the categories below:

a. sexual life

b. race

c. religion

d. political opinions

e. trade union membership

f. physical and mental health

g. commission or alleged commission of any offence

h. proceedings, disposals and sentence in relation to the commission or alleged commission of any offence

3.8 **Third party:** any person or organisation other than the data subject, data controller or data processor.

4 Associated documents and guidance

4.1 The University also publishes data protection-related policies and guidelines, which includes guidance and advice for staff on the following areas:

a. **collecting and processing personal data:** appropriate Policy Doc; Data Protection Privacy Impact Assessment Policy and guidance, Data Processing Contract template and checklist

b. **disclosing personal data:** Subject access Rights Procedure, Data Sharing guidance

c. **the retention and disposal of personal data:** Retention Schedule & File Storage Policy

d. **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 Governance and Assurance Policy defines roles for System Owners to safeguard personal and sensitive data.

e. **managing information security breaches:** Data Breach Policy

5 Areas of responsibility

5.1 The DPA 2018 and the UK 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 2018 and is obliged to ensure that the DPA 2018 requirements are implemented, monitored and evaluated.

A University Leadership Team

5.2 The University Leadership Team (ULT) have overall responsibility for ensuring that the organisation complies with its legal obligations.

B University Senior Information Risk Owner

5.3 The University Secretary, Registrar and Chief Compliance Officer (USRCCO) is the University Senior Information Risk Owner (RISO) 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.

C Information Governance Committee

5.4 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

a. information assurance
b. data quality management
c. information and data ownership
d. information management policy
e. information risk management
f. information breach management
g. recommendations as to required training
h. data sharing

5.5 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 Data Protection Officer (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.

D Data Protection Officer

5.6 The DPO is responsible for monitoring internal compliance with data protection legislation. Their responsibilities include

a. briefing IGC on their data protection responsibilities
b. dealing with all correspondence between the University and the Information Commissioner's Office (ICO)
c. reviewing and updating data protection and related policies and obtaining approval from IGC and ULT
d. providing specialist advice to staff on data protection issues, including data protection breaches
e. manage and deal with subject access requests and bringing issues to the attention of the USRCCO
f. update and maintain a record of processing activity (RoPA) under Article 30 of the UK GDPR

E Communications

5.7 The Executive Director, External Relations, Student Recruitment and Communications or delegate is responsible for approving any statements on publicity materials or similar releases with an impact on data protection or privacy.

F Staff

5.8 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 2018 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.

G Students

5.9 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.

5.10 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.

H Volunteers and third parties

5.11 Volunteers are expected to abide by this policy and its associated documents.

5.12 Volunteers processing personal information will also be expected to undertake mandatory training.

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

6 Principles

6.1 The UK 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:

A Lawfulness, fairness & transparency

6.2 Personal data should be processed lawfully, fairly and in a transparent manner.

6.3 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.

6.4 For data to be processed lawfully, one of the legal bases—as set out in Data Protection Law—must apply:

a. **Consent:** Consent must be freely given, specific, informed and unambiguous

b. **Contract:** Necessary for fulfilling a contract or to enter into a contract

c. **Legal obligation:** Necessary to comply with the law

d. **Public task:** Necessary to perform a task in the public interest or for an official function

e. **Legitimate interests:** Necessary for the University's legitimate interests or the legitimate interest of another party, unless it would undermine the interests of an individual's right to privacy

f. **Vital interests:** Necessary to protect the life of the individual or another individual

6.5 There are additional safeguards when processing sensitive special category data. See

B Purpose limitation

6.6 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) of the UK GDPR, not be considered to be incompatible with the initial purposes ('purpose limitation').

C Data minimisation

6.7 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.

D Accuracy

6.8 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 is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

E Storage limitation

6.9 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.

6.10 When no longer needed for the purpose for which collected and if there is no lawful basis to continue to retain the personal data must be either fully anonymised or deleted in accordance with University Retention Schedule.

F Security

6.11 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.

G Accountability

6.12 The Controller shall be responsible for, and be able to demonstrate compliance with, Article 5(1) of the UK GDPR.

7 Training

7.1 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 both the 'Data Protection' and 'Cyber Security' online learning modules. 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

A Subject access

8.1 The University 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 and the right of access to that data and receive copies of their Personal Data.

8.2 Individuals also have the additional rights:

a. **The right to rectification:** to have inaccurate personal data rectified or completed.

b. **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.

B Direct marketing

8.3 The University will comply with the requirements of the 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.

8.4 All telephone numbers will be screened against the TPS prior to a relevant marketing call being made.

8.5 A privacy notice will be provided to all individuals at the time this consent is recorded.

C Right to object

8.6 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:

a. the Subject has consented to the processing

b. the processing is necessary:

[i] in relation to a contract that the Subject has entered into

[ii] because the Subject has asked for something to be done so they can enter into a contract

c. the processing is necessary because of a legal obligation that applies to the University (other than a contractual obligation)

d. the processing is necessary to protect the Subject's 'vital interests'

8.7 Any such objections should be addressed to the DPO and must specify the reason why the processing has this effect.

D Right to have personal data rectified, blocked, erased or destroyed

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

9 Audit and assurance

A Privacy by design: Data Protection Impact Assessment (DPIA)

9.1 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.

B Data Protection Audit

9.2 The DPO 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 DPA 2018 and the security of our systems is complied with.

10 Sanctions

10.1 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.

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

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

a. 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

b. unauthorised access to, and/or modification of, computer material.

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

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

11 Review

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

12 Appendix A: Appropriate Policy Document

12.1 The University of Hull is committed to protecting all personal data that we process.

12.2 We ensure processing is compliant with the UK GDPR, the DPA 2018 and any associated legislation.

12.3 Schedule 1, Part 4 of the DPA 2018 outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

12.4 The University as a Higher Education provider will process SC and CO data as below

a. racial/ethnic origin

b. political opinions

c. religious or philosophical beliefs

d. trade union membership

e. genetic and biometric data

f. data concerning health

g. data concerning sexual life or sexual orientation

h. criminal offence data

12.5 In order to process these categories, the University, in addition to an Article 6 UK GDPR condition, must rely on an Article 9 UK GDPR Condition for processing and Article 10 in respect of Criminal conviction data. The University also has to recognise a valid condition within Schedule 1, Part 1, 2 or 3.

12.6 Section 10 of the DPA 2018 clarifies under which Article 9 conditions we must also be able to identify an appropriate Schedule 1 condition.

12.7 The Schedule 1 conditions upon which we rely and of which this document covers:

a. Part 1, paragraph 1, ***Employment, social security and social protection***: where the University needs to process SC/CO data for the purposes of performing its obligations or rights as an employer, or for guaranteeing the social protection of individuals. This includes our health and safety responsibilities

b. Part 2, paragraph 6, ***Statutory etc and government purposes:*** where the University needs to process SC/CO data to comply with our statutory obligations

c. Part 2, paragraph 8, ***Equality of opportunity or treatment:*** where the University needs to process SC/CO data for the purposes of monitoring equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained

d. Part 2, paragraph 10, ***Preventing etc unlawful acts:*** where the University needs to process CO data for the purpose of preventing or detecting unlawful acts and obtaining consent would prejudice those purposes, and the processing is necessary for reasons of substantial public interest

e. Part 2, paragraph 11, ***Protecting the public against dishonesty etc:*** where the University needs to process CO data to protect members of the public from malpractice, unfitness, incompetence or mismanagement in the administration of a body or organisation, and obtaining consent would prejudice the exercise of the

protective function, and the processing is necessary for reasons of substantial public interest

f. Part 2, paragraph 12, ***Regulatory requirements relating to unlawful acts and dishonesty etc:*** where the University needs to process CO data to comply with a requirement which involves taking steps to establish whether an individual has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct, and the processing is necessary for reasons of substantial public interest

g. Part 2, paragraph 17, ***Counselling etc:*** where the University needs to process SC/CO data in order to provide confidential counselling, advice or support or of another similar service provided confidentially, only where, in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining consent would prejudice the provision of the service, and the processing is necessary for reasons of substantial public interest

h. Part 2, paragraph 18, ***Safeguarding of children and of individuals at risk:*** where the University needs to process SC/CO data in order to protect the physical, mental or emotional well-being of an individual under the age of 18, or over the age of 18 and at risk, only where, in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining the data subject's consent would prejudice the provision of the protection, and the processing is necessary for reasons of substantial public interest

A Accountability

12.8 We demonstrate our compliance with the data protection principles provided in Article 5 of the UK GDPR through the following measures and documents:

a. We have an appointed DPO whose role and responsibilities align with the provisions of Chapter IV, Section 4 of the UK GDPR.

b. We hold a RoPA setting out the personal data categories we process, the purposes, the lawful basis, retention and recipients and security requirements.

c. We have privacy notices in place to explain to individuals how and why their data is processed making clear their rights in relation to that data.

d. We carry out DPIAs for uses of personal data that are likely to result in risk to individuals.

e. When we routinely share data with third parties, we enter into written agreements with Controllers or processors in accordance with Article 26 and 28 of the UK GDPR.

f. We implement appropriate security measures proportionate to the risk associated with the processing.

B The Principles

12.9 When processing special category personal data and criminal conviction data the University will comply with the data protection principles.

12.10 **Processing is lawful, fair and transparent:** The appropriate lawful basis for processing

is stated in the University's privacy notices outlining the processing, unless a valid exemption from the right to be informed is applicable.

12.11 **Processing is for specified purposes; no further processing that is incompatible with those specified purposes:** Personal data will only be processed for the specific purposes notified to the data subject via a privacy notice or for any other purposes permitted under data protection legislation. Personal data will not be collected for one purpose and then used for a separate, unrelated purpose. Should it become necessary to change the purpose to something incompatible with the original purpose for which the data is processed, data subjects will be informed of the new purpose before any processing occurs.

12.12 **Processing is adequate, relevant and limited to what is necessary for the purpose:** Only the minimum personal data needed to fulfil the specified purpose will be collected, information which is not needed or is not relevant to the purpose will not be collected or otherwise processed.

12.13 **Personal data is accurate and kept up to date:** Where the University has been notified that information is incorrect, steps will be taken to correct it. Accuracy of personal data will be checked at the point of collection and reviewed at necessary intervals.

12.14 **Personal data is kept no longer than is necessary:** Personal data will be managed in line with the University's Retention Policy & Retention Schedule, which details how long certain types of information should be retained and when and how it should be securely destroyed. Retention periods are based on both legal and operational requirements.

12.15 Any information about criminal convictions of staff or students obtained as part of a DBS check will be retained in accordance with DBS standards.

12.16 **Processing is carried out securely to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage:** Personal data is stored securely using appropriate technological controls with access restricted both internally and externally on a need-to-know basis. The University will ensure that appropriate technical and organisational measures are taken to protect against unlawful or unauthorised processing of personal data and against its accidental loss, destruction or damage.

12.17 It is the responsibility of all University staff to adhere to this Appropriate Policy Document when processing such personal data.

12.18 All staff and those with approved access to University information and systems must complete annual mandatory Information Security Training. Any suspected or actual misuse, unauthorised disclosure of, or access to, personal data must be immediately reported to the DPO.