UNIVERSITY OF HULL

Data Protection

Data Protection Policy

Approved by: University Leadership Team
Scope: This Policy applies to all University Staff, Students, Contractors and volunteers working for the University.
With effect from: January 2018 **Next date for review:** January 2019
Other related policies: To be read in conjunction with the
Contact for further information: Data Protection Officer Dataprotection@hull.ac.uk
Reference to any superseded policy/amalgamations: Supersedes previous Data Protection Policy
Relevant legal framework : Data Protection Act 2018 EU General Data Protection Regulations 2018
Equality analysis: The implementation of this policy is not considered to have a negative impact on protected characteristics.
Freedom of information: This Policy is publicly available through the University's Publication Scheme under the Freedom of Information Act 2000

Version	Changes
3.0	

Table of Contents

1. Introduction

The University of Hull's Data Protection Policy has been produced to ensure its compliance with the Data Protection Act 2018 and the EU General Protection Regulations 2018(DPA and). The Policy is intended to complement the University's Data Protection Statement and incorporates guidance from the Information Commissioner's Office (ICO) and other relevant organisations. **Definitions**

Explicit Consent – freely given, and informed, indication by which the data subject signifies their wishes.

Data – Information which is (or intended to be) processed by a computer or recorded in a filing system, or any other information held by a public authority.

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

Data Controller – An organisation that has control of personal data and/or sensitive personal data.

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

Personal Data – Information relating to a living and identifiable individual.

Process – to obtain, store, hold, disclose, etc., personal information. It is hard to think of anything that could be done with or to personal data (in this case images) that would amounts to processing.

Special Category 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.

2. Associated Documents and Guidance

The University has also published further policies which provide guidance and advice for staff on the following areas:

*** the retention and disposal of personal data;** The Policy and Schedule on Data Retention can be found on the Information Governance SharePoint site

*****

*** managing information security breaches;** The Policy on how to deal with a data breach can be found on the Information Governance SharePoint site

*** Data Privacy Impact Assessments;** The Policy on Data Privacy Impact Assessments can be found on the Information Governance SharePoint site.

*** Consent, subject access, anonymization;** The Data Subject's Rights Policy can be found on the Information Governance SharePoint site.

3. Who is responsible?

The Data Protection Act 2018 (DPA) applies to all staff, students, contractors and volunteers working for the University. The University is a Data Controller, as defined in Article 4 (7) GDPR 2018, and is obliged to ensure that the DPA's requirements are implemented, monitored and evaluated.

3.1. University Leadership Team

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

3.2. University Senior Information Risk Owner (SIRO)

The University Registrar and Secretary is the University Senior Information Risk Owner (SIRO) and takes responsibility for operating a framework for assessing risks to information across the organisation, and approving unusual or controversial disclosures of personal data to other organisations.

3.3. Information Governance Committee

The primary function of the Information Governance Committee 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; and,
- Recommendations as to required training.

.

3.4. 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.

4.4.1 Executive Senior Information Risk Owners

Executive SIROs will assume responsibility for University information systems within their remit. 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.

4.4.2 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; and
- escalate risks to information to their Executive SIRO as necessary

4.4.3 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; and,
- work with Data Protection and Information Security specialists to assess risks to information, and how those risks can be managed.

3.5. Communications / PR

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

3.6. Managers

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

3.7. 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.

Any personal information that staff provide to the University must be accurate and kept up-to-date by notifying the University of any alterations to address and personal details.

3.8. 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.

3.9. 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.

4. The Data Protection Principles

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

1. Personal data shall be:

   a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

   b. 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');

   c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

   d. 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');

   e. 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');

   f. 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').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

5.Responsibilities

University staff who process personal data as part of their duties must ensure that they are complying with the six data protection principles described in section 5 Processing data is a collective term for any action taken relating to personal data and includes obtaining, recording, storing, using, sharing, disclosing, transferring, and destroying data.

5.1 Obtaining Personal Data

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

2. 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 (see section 11). If it is not they should notify the Information Compliance Officer before any personal data is collected so that the notification can be amended.

3. 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

4. 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.

5. Data must be collected in a secure manner

5.2 Recording Personal Data

1. 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.

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

3. 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.

5.3 Storing Personal Data

1. All staff whose work involves processing personal data, whether in electronic or

paper format, must take personal responsibility for its secure storage.

2. 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.

3. Personal data in paper format must be kept in a locked filing cabinet, cupboard or drawer.

4. 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.

5. 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.

6. 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.

7. Staff must not keep sensitive personal data (see section 2.2) on portable storage devices unless they have received authorisation from both their line manager and the Information Compliance Officer.

8. 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 (see section 2.2) the authorisation of their line manager and the Information Compliance Officer is required.

5.4 Using Personal Data

1. Personal data should only be processed for the specific purpose contained in the privacy notice provided when the data was collected.

2. If staff wish to use the personal data in a new and unforeseen way a Data Privacy Impact Assessment will need to be undertaken In certain cases clear consent from the data subjects must be obtained before the personal data is used in the new way.

3. Personal data should only be used for marketing activities where data subjects have given their consent. Unsolicited marketing activities involving messages sent by telephone, fax, email or text must conform to the Privacy and Electronic Communications Regulations 2003 (PECR).

4. Particularly in open plan offices, staff should be aware of the possible risk of unauthorised persons viewing personal data displayed on computer screens or in

paper documents. Preventative measures such as facing computer screens away from high traffic or public areas and taking care not to leave documents containing personal data in view should be taken. The use of privacy filters on computer screens should also be considered.

5.5 Sharing and Disclosing Personal Data

1. When personal data is shared between University departments for valid business reasons the data must be relevant and the minimum necessary to achieve the objective. Consideration must be given to the appropriate level of security required when transferring data and to other anticipated risks. Departments must assess whether any new use of the data will be compatible with the purpose for which it was originally collected. If it is not the data subjects may need to be made aware of the intention to use their data in this way and in some instances consent may be required. Departments must also consider the retention and disposal of the shared information. Where the data is required for a single purpose the duplicate information should be destroyed after use. Where a permanent record is required the departments must establish a process to ensure the data continues to be held in line with the data protection principles. Further guidance on sharing data internally is available from the Information Compliance Officer.

2. In some instances the University is required for mandatory or statutory reasons to share information with certain third parties. Personal data may also be shared with other third parties if there is a clear and lawful purpose for doing so, if the data sharing is a proportionate means of achieving that purpose and if the data sharing is transparent to the data subjects. Further guidance on sharing data with third parties is available from the Information Compliance Officer.

3. The University, as the data controller, continues to remain liable for ensuring that data processing complies with the eight data protection principles when the processing is undertaken by an external company or organisation (known as a data processor). If a Faculty or Service department decides to outsource a data processing function, it must ensure that a Data Processing Agreement is in place first to provide assurance that the data processor will act in accordance with the DPA. The Information Compliance Officer should be made aware of any intention to engage a data processor so that guidance on Data Processing Agreements can be provided. When finalised, a signed copy of the Data Processor Agreement should be sent to the Information Compliance Officer to hold on file.

4. The DPA 18 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Staff who receive a request to disclose personal data for reasons relating to national security, crime and taxation should contact the Information Compliance Officer for advice and so that the request can be recorded.

5. In response to other requests, in most cases, staff must not disclose personal data, particularly sensitive data, without the consent of the data subject. If consent is received, staff must ensure that the data is given to the correct enquirer and for this reason disclosure should be made in writing and not by telephone.

6. If personal information is requested by a data subject or by a third party that is not provided as part of the normal course of business, the individual who is requesting

the data should be directed to the Information Compliance Officer for advice on how to make a Subject Access Request (SAR). The University must respond to SARs within forty calendar days of receiving the request.

5.6 Transferring Personal Data

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

2. 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.

3. 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.

4. 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.

5. 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.

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

7. 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 (see section 2.2). As stated in 4.3.6, personal data stored on portable devices must also be encrypted.

8. 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.

9. Personal data should not be sent or received by fax except where it is absolutely necessary. Where the use of a fax machine is unavoidable, the fax cover sheet should be marked confidential and a ring ahead procedure should be agreed to ensure the receiving machine is being monitored. The fax number should be dialled manually rather than using automated dialling or stored numbers. Safe receipt of the fax should be acknowledged by the recipient and any fax reports retained. Inbound

faxes should be removed from the fax machine promptly and dealt with appropriately.

.

6.Data Security

It is the policy of the University of Hull that the security and confidentiality of Personal Data shall be maintained at all times in accordance with Artilce 5(f) GDPR
To this end, the University requires all staff that use University IT systems (including email) that may contain personal data to complete mandatory Information Security and Data Protection Training. Completion of additional, or alternative, training may be required for specific roles depending on an assessment of risk.

Examples of some of the organisational and technical measures that should be employed to maintain Information Security are detailed in the Data Protection Guidelines.

6.1 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.
.

.

7. Sanction

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

8. Review

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

9.Appendix A – Article 6 and 9 Conditions

Article 6 conditions

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

2. (a) The data subject has given consent to the processing of his or her personal

data for one or more specific purposes;

3. (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

4. (c) Processing is necessary for compliance with a legal obligation to which the controller is subject;

5. (d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

6. (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

7. (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

8. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 9 Conditions

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

    a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

    b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

    c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject;

f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.