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: Information Compliance Officer – infocompliance@hull.ac.uk
Reference to any superseded policy/amalgamations: Supersedes previous Data Protection Policy
Relevant legal framework : Data Protection Act 1998
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
2.0	

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 1998 (DPA and associated legislation. 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. This Policy should be read in conjunction with the Data Protection Guidelines.

2. 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 organization 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.

Sensitive Personal 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.

3. Associated Documents and Guidance

The University also publishes Data Protection Guidelines, which includes guidance and advice for staff on the following areas:

*** collecting and processing personal data** (including privacy notice checklist, third party data processing checklist, undertaking research involving the gathering of personal data and processing photographs, videos and CCTV);

*** disclosing personal data** (including managing requests for personal information from third parties and managing subject access requests);

*** the retention and disposal of personal data;**

*** keeping personal data secure** (including, faxing personal data safely, e-mailing 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;**

*** transferring personal data outside the European Economic Area (EEA); and,**

*** Frequently Asked Questions.**

4. Who is responsible?

The Data Protection Act 1998 (DPA) applies to all staff, students, contractors and volunteers working for the University. The University is a Data Controller, as defined in Section 1 of the DPA, and is obliged to ensure that the DPA's requirements are implemented, monitored and evaluated.

4.1. University Executive Group

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

4.2. 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.

4.3. Information Governance Working Group

The primary function of the Information Governance working group 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.

The working group will report, and make recommendations, to the Information Advisory Group (IAG) for endorsement and, where appropriate, submission for decision by the University Executive Group.

4.4. Information Compliance Officer

The officer in day-to-day control of Data Protection is the Information Compliance Officer. Their responsibilities include:

- Briefing the Senior Management Group 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 the Senior Management Group;
- Providing specialist advice to staff on Data Protection issues;
- Ensuring that Data Protection induction and training takes place;
- Overseeing subject access requests and bringing issues to the attention of the University Registrar and Secretary;
- Advising on Records Management;
- Overseeing implementation of the Records Management Policy and bringing issues to the attention of the University Registrar and Secretary;
- Planning, undertaking or commissioning data protection audits.

4.5. 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 Working Group.

4.5.1 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.

4.5.2 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

4.5.3 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.

4.6. 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.

4.7. 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.

4.8. 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.

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.

4.9. 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.

4.10. 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 Guidelines.

5. 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 processed fairly and lawfully, and will not be processed unless:
    a. One of the Conditions from Schedule 2 (Appendix A) of the DPA is met
    b. In the case of Sensitive Personal Data, one of the conditions from Schedule 3 (Appendix A) is also met.
2. Personal data shall be obtained/processed for specific lawful purposes.
3. Personal data held must be adequate, relevant and not excessive.
4. Personal data must be accurate and kept up to date.
5. Personal data shall not be kept for longer than necessary.
6. Personal data shall be processed in accordance with rights of data subjects.
7. Personal data must be kept secure.
8. Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection for that data.

6.Responsibilities

University staff who process personal data as part of their duties must ensure that they are complying with the eight 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.

6.1 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 Information Compliance 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

6.2 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 any retention period specified in the relevant privacy notice.

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.

6.3 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 Helpdesk 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.

6.4 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 the privacy notice should be updated to reflect the change. If the change would not reasonably be expected by the data subjects, staff must actively communicate the revised privacy notice to them. 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.

6.5 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 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.

6.6 Transferring Personal Data

1. Any transfer of personal data must be done securely and in line with the University's Information Systems Acceptable Use Policy.

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.

6.7 Destroying Personal Data

1. All departments should have a local record retention schedule for the personal data they hold and ensure that data is destroyed when it is no longer required. The record retention schedule should be in accordance with the retention periods specified in privacy notices. Further guidance about record retention schedules is available from the Information Compliance Officer.

2. Personal data in paper format must be shredded or sealed in the confidential waste bags provided by the Estates and Facilities Department. Personal data in electronic format should be deleted. Disks that hold personal data can be destroyed by the ICT department if office shredders do not include this facility.

7.Subject Rights

7.1Subject Access

The University of Hull acknowledges and respects that Data Subjects (whatever their relationship with the University) have the right to request copies of their Personal Data. More information on this process can be found on the University website contained with the privacy notice.

7.2 Direct Marketing

The University of Hull will comply with the requirements of the Privacy and Electronic Communications Regulations 2003 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.

7.3 Processing Causing Damage and Distress

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 Information Compliance Officer (infocompliance@hull.ac.uk) and must specify the reason why the processing has this effect.

7.4 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.

8.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 Principle Seven of the DPA.

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 at section 6 of the Data Protection Guidelines.

8.1 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.

8.2 Anonymisation and Pseudonymisation

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 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.

9. Audit and Assurance

9.1 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 a DPIA is required. The DPIA Policy has the necessary templates for this.

9.2 Data Protection Audit

The Information Compliance Officer 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 is complied with.

10. Registration and Notification

As a data controller, the University is required to register with the ICO and submit an annual notification listing the purposes under which it processes personal information. The University must also notify the ICO within 28 days should any entry become inaccurate or incomplete. The ICO publishes a register of data controllers on its website which is available to the public for inspection. The University's notification can be found on the ICO's website by entering its registration number which is Z7846984.

It is an offence for the University to process personal data that falls outside of the purposes declared in its notification. Staff who work with personal data should be familiar with the University's notification and inform the Information Compliance Officer if they intend to implement changes that may require the notification to be amended.

11. Sanction

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 55 of the Data Protection Act 1998 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

- 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.

12.Review

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

13.Appendix A – Schedule 2 & 3 Conditions

Schedule 2 Conditions

1. The individual whom the personal data is about has consented to the processing
2. The processing is necessary:
   - in relation to a contract which the individual has entered into; or
   - because the individual has asked for something to be done so they can enter into a contract.
3. The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
4. The processing is necessary to protect the individual's "vital interests".
5. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
6. The processing is in accordance with the "legitimate interests" condition.

Schedule 3 Conditions

1. The individual whom the sensitive personal data is about has given explicit consent to the processing.
2. The processing is necessary so that you can comply with employment law.
3. The processing is necessary to protect the vital interests of:

- the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
- another person (in a case where the individual's consent has been unreasonably withheld).

4. The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
5. The individual has deliberately made the information public.
6. The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.

7. The processing is necessary for administering justice, or for exercising statutory or governmental functions.
8. The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
9. The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.
10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.