LIVERPOOL HOPE UNIVERSITY

Est. 1844

Data Protection Policy

Document Control

Responsibility for Policy:	Legal Services Governance and Risk Senior Officer
Approved by and date:	University Council 22nd November 2023
Frequency of Review:	Every 5 years
Next Review date:	November 2028
Related Policies:	Information Management Policy Information Security Policy IT Services Acceptable Use Policy Data Breach Procedure Retention Schedules
Minor Revisions:	N/A
EIA:	N/A

1. Purpose and Scope

1.1. The purpose of this policy is to ensure compliance with the UK General Data Protection Regulations, related legislation and guidance ('Data Protection law'). Data Protection law is concerned with protecting personal data. Personal data is information about who you are, where you live, what you do and more. It is any and all information that identifies you as a data subject, such as:

- people's names and addresses;
- photographs;
- staff or student reference numbers;
- medical information;
- academic information
- reports.

.

If a document, file or image identifies a person, or could be used in combination with other information to identify them, then it is personal data. This applies even if the information does not include a person's name.

Some personal data is more sensitive and is afforded more protection. This is information related to: race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric ID data; health data; sexual life and/or sexual orientation; and criminal data (convictions and offences). However, information is only personal data if it relates to someone who is alive. Data protection laws do not apply after someone has died.

Processing personal data means taking any action in relation to someone's personal data; it includes storing, handling, recording, making changes to the data held, sharing and re-organising the way data is held.

The University is a data controller, meaning it has responsibility for deciding how personal data is processed and protecting it from harm. Occasionally, the University may delegate the processing of personal data to data processors, but the responsibility for keeping it safe will still rest with the University as the data controller. On rare occasions the University may operate as a data processor, where the data controller is an external agency.

1.2. This policy applies to all staff except when acting in a private or non-University capacity. In this policy, the term 'staff' means anyone working in any context within the University at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, retired but active, research staff, other visiting research or teaching staff, workers, trainees, interns, seconded staff, agency staff, agents, volunteers, and external members of committees. This policy also applies to third parties associated with the University, such as research collaborators.

1.3. This policy applies to all students when processing personal data on behalf of the University, but not in any other situation including when acting in a private or non-University capacity.

1.4. All processing of personal data by third parties on behalf of the University, where the University is data controller, shall be covered by contract and include adequate data protection clauses.

1.5. This policy is not, and should not be confused with, a privacy notice (a statement informing data subjects how their personal data is used by the University). Privacy notices can be found here:

https://www.hope.ac.uk/aboutus/governance/generaldataprotectionregulations/privacynotices/

1.6. This policy should be read in conjunction with the obligations in the following documents, which supplement this policy where applicable:

1.6.1. staff employment contracts, which impose confidentiality and responsibility obligations in respect of information held by the University;
1.6.2. information security policies, procedures and terms and conditions, which concern the confidentiality, integrity and availability of University information, and which include rules about acceptable use, breach reporting, IT monitoring, and the use of personal mobile devices;
1.6.3. records management policies and guidance, which govern the appropriate retention and destruction of University information;
1.6.4. any other contractual obligations on the University or individual staff which impose confidentiality or data management obligations in respect of information held by the University, which may at times exceed the obligations of this and/or other policies in specific ways (e.g. in relation to storage or security requirements for funded research).

2. Policy Statement

2.1. The University is committed to complying with data protection law as part of everyday working practices. Members of the Hope community will be required to carry out relevant and appropriate data protection training; the level, frequency and nature of the training is determined by the Personnel Department.

2.2. The University will comply with the six data protection principles. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- adequate, relevant, and limited to what is necessary;
- accurate and, where necessary, up to date;
- not kept for longer than necessary; and
- kept safe and secure**.**

2.3. The University has a corporate responsibility as a data controller (or when acting as a joint data controller or a data processor) for:

2.3.1. understanding, and applying as necessary, the data protection principles[i] when processing personal data;
2.3.2. understanding, and fulfilling as necessary, the rights given to data subjects[ii] under data protection law;

2.3.3. understanding, and implementing as necessary, the University's accountability obligations[iii] under data protection law.
2.3.4. complying with data protection law and holding records demonstrating this;

2.3.5. cooperating with the Information Commissioner's Office (ICO) as the UK regulator of data protection law; and
2.3.6. responding to regulatory/court action and paying administrative levies and fines issued by the ICO.

3. Roles and Responsibilities

3.1. The University shall designate a Chief Information Officer and a Data Protection Officer (DPO) with the ability to fulfil the tasks required by law. The University shall enable the effective performance of their tasks and ensure that the DPO is given sufficient autonomy, time, resources and support to carry out their tasks effectively, including active support by senior management. The DPO is an advisory role and is concerned with the University's compliance with data protection legislation.

3.2. **The Chief Information Officer in consultation with the Data Protection Officer** shall:

3.2.1. provide advice, assistance and recommendations to Senior Management in relation to data protection risks;
3.2.2. enable compliance with data protection legislation;
3.2.3. play a key role in fostering a data protection culture within the University and provide advice when required;
3.2.4. review the planning, implementation and progress of the University's data protection initiatives periodically, reporting to Council;
3.2.5. Inform the University's Senior Executive Team of breaches of data protection legislation as necessary;
3.2.6. be the University's point of contact with the Information Commissioner's Office.

3.3. The DPO shall not determine the purposes of processing personal data, or the means by which any personal data processing activity is done. The DPO shall provide advice when sought.

3.4. **University Council** is responsible for:

3.4.1. reviewing (at least once every five years) and approving this policy; and
3.4.2. assessing the overall risk profile and ensuring appropriate resources and processes are in place and implemented to enable compliance with data protection law.

3.5. **The University Senior Executive Team (USET)** shall have overall responsibility

3.5.1. to ensure that the purposes and means of processing of personal data for which the University is data controller are determined in compliance with legislation.

3.5.2. for ensuring implementation of and compliance with this policy in accordance with the University's line management structure.

3.6. **Managers and Heads of Department** shall have management responsibility for:

3.6.1. the processing of personal data (of which the University is data controller) in compliance with data protection law, including the appropriate determination

of the purposes of processing personal data, and the means by which any personal data processing activity is carried out.

3.6.2. the identification and management of data protection risks

3.6.3. planning, implementing and progressing the University's data protection initiatives

3.6.4. managing the implementation of essential elements of data protection legislation, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing and notification and communication of data breaches

3.6.5. managing the response to breaches of data protection legislation in consultation with the Data Protection Officer

3.6.6. ensuring that no individual is given access to personal data without having undertaken appropriate training, reading relevant policy and guidance and taking advice from the DPO as required.

3.6.7. play a key role in fostering a data protection culture within the University.

3.6.8. ensure that local processes and procedures are developed, implemented, followed and regularly reviewed

3.6.9. monitor and report on compliance in their business units as required by the University.

3.7. The roles and responsibilities above do not waive any personal liability for individual criminal offences[iv] for the wilful misuse of personal data under data protection law.

4. Training

The University is committed to complying with data protection law as part of everyday working practices. All staff members will receive training on data protection that is proportionate and relevant to the role performed. The level, frequency and nature of the training is determined by the Personnel Department.

5. Data Retention

All data shall be retained safely, securely and in accordance with the law, regulatory requirements and University Retention Schedules, available at: https://www.hope.ac.uk/aboutus/governance/generaldataprotectionregulations/

6. Breach

6.1. All breaches of this policy and data protection legislation shall be reported immediately in accordance with the Breach Reporting Procedure: https://www.hope.ac.uk/media/aboutus/governancedocuments/GDPR%20Data%20Breach%20Procedure.pdf. Third parties shall report via their University point of contact.

Some breaches may be reportable to the Information Commissioner's Office (ICO).The decision to report is made by the DPO depending on the risk to people's rights and freedoms. The DPO will consult with the USET before notifying the ICO.

6.2. The University wishes to encourage data breach reporting in order to ensure breaches are dealt with correctly, promptly and lessons can be learnt. However, it is possible that a breach of this policy by an employee or student may result in disciplinary action. A breach by a third party may result in a termination of contract and/or compensation claim.

7. Information Rights

7.1. Data subjects have rights to be informed of: access; rectification; erasure; restriction; data portability; and objection.

7.2. We have an established processes to handle subject access requests and other information rights requests. Please send Freedom of Information requests and Data Subject Access Requests to caseworker@hope.ac.uk

For more information regarding the University's approach to data protection please visit http://www.hope.ac.uk/aboutus/governance/generaldataprotectionregulations/

For general data protection information www.ico.org.uk