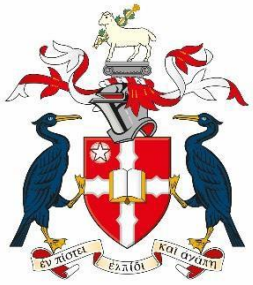

LIVERPOOL HOPE UNIVERSITY

Liverpool Hope University

Data Protection Policy

This replaces the Data Protection Policy approved on 26th November 2013	
Approved by:	University Council
Date Approved:	10th July 2018

1. Purpose and Scope

1.1. The purpose of this policy is to ensure compliance with the General Data Protection Regulation and related EU and national legislation ('data protection law'). Data protection law applies to the storing or handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects').

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).

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 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. As such all relevant members of staff will be required to carry out (as a minimum) an online data protection training module.

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

2.2.1. understanding, and applying as necessary, the data protection principles[i] when processing personal data;

2.2.2. understanding, and fulfilling as necessary, the rights given to data subjects[ii] under data protection law;

2.2.3. understanding, and implementing as necessary, the University's accountability obligations[iii] under data protection law.

2.2.4. complying with data protection law and holding records demonstrating this;

2.2.5. cooperating with the Information Commissioner's Office (ICO) as the UK regulator of data protection law; and

2.2.6. 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 Data Protection Officer (DPO) with the ability to fulfil the tasks referred to in Article 39. The University shall enable the effective performance of the DPO's 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 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

3.2.4. review the planning, implementation and progress of the University's data protection initiatives periodically, reporting to Council

3.2.5. advise Rectorate Team in relation to any breaches of data protection legislation

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.

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. **Rectorate Team** 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 will be 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 done

3.6.2. the 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

3.6.6. ensuring that no individual is given access to personal data without having undertaken appropriate training and read relevant policy and guidance.

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. Breach

4.1.1. All breaches of this policy and data protection legislation shall be reported immediately in accordance with the Breach Reporting Procedure. Third parties shall report via their University point of contact.

4.1.2. 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.

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

[i] The principles in relation to personal data are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

[ii] The data subject rights are: to be informed; access; rectification; erasure; restriction; data portability; and objection (including in relation to automated decision-making).

[iii] The accountability obligations include: implementing appropriate data protection policies; implementing data protection by design and default in projects, procurement and systems; using appropriate contracts with third party data controllers and data processors; holding relevant records about personal data processing; implementing appropriate technical and organisational security measures to protect personal data; reporting certain personal data breaches to the Information Commissioner's Office; conducting Data Protection Impact Assessments where required; and ensuring adequate levels of protection when transferring personal data outside the European Economic Area

[iv] These criminal offences include: unlawfully obtaining, disclosing or retaining personal data; recklessly re-identifying de-identified personal data without the data controller's consent; deliberately altering or deleting personal data to prevent disclosure in accordance with data subject access rights; forcing a data subject to exercise their access rights; and knowingly giving false statements to the ICO.

LIVERPOOL HOPE UNIVERSITY
1844

LIVERPOOL HOPE UNIVERSITY

THE GENERAL DATA PROTECTION REGULATIONS – DOS AND DON'TS

DON'T use data for any reason other than what it was originally collected for.

DON'T leave data unattended. Keep a clear desk, tidy confidential data away when not in use.

DO consider whether it's necessary to use personal data to achieve your objective.

DON'T collect or allow others to access personal data 'just in case'. Collect or use the minimum amount of personal data as needed for your specific objective.

DO Ensure that data is accurate and up to date. For this aim use centralised sources of data where possible, this will also avoid creating unnecessary copies of the same information.

DO Anonymise or pseudonimise data where possible.

DON'T keep data for longer than is necessary. Do regularly and securely destroy out of date information and data that is no longer required in paper form or electronic records. Check what the retention period is for the data you're storing.

DO encrypt attachments or password protect large volumes or special category data if sending electronically.

DO make sure you have the sender's permission to share/forward their name or address when using email or use the blind copy function so recipients can't identify each other.

DON'T write any comment about any individual that is unfair or untrue and that you would not be able to defend if challenged. You must assume that anything that you write about a person will be seen by that person.

DON'T share data with other teams or departments unless there is a genuine business need to access personal data. Establish a way to share data securely.

DON'T share personal data with external agencies or third parties (eg parents) unless you are sure that there is a legal basis for doing so.

DON'T store personal data on your own personal devices or on USB sticks. DO use secure areas provided by the University for working on and storing personal data.

DON'T use cloud based systems to store personal data, unless security controls for that system have been reviewed by IT Services.

DO be particularly careful when dealing with special category data: eg data concerning race or ethnic origin, political opinion, religious belief, sexual life, criminal offences, trade union membership, health.

DO report any breach/loss of personal data to the Head of Legal Services, Governance and Risk immediately. The University only has 72 hours to notify the Information Commissioner's Office.

DO take time to complete the University training on Data Protection and access the Staff Guidance Book at http://www.hope.ac.uk/aboutus/governance/dataprotection/