

## Data Protection Policy

<b>Responsibility for Policy:</b>	University Secretary and General Counsel
<b>Relevant to:</b>	All Staff, Governors, sub contractor's apprentices, work placements and interns, Students and Academic Partnerships
<b>Approved by:</b>	ELT, 5 <sup>th</sup> September 2019
<b>Responsibility for Document Review:</b>	Data Protection Officer
<b>Date introduced:</b>	2005
<b>Date(s) modified:</b>	April 2008, December 2008, September 2010, July 2013, May 2014, January 2015, January 2016, August 2016, September 2017, September 2018, September 2019, September 2020
<b>Next Review Date:</b>	September 2021

### RELEVANT DOCUMENTS

- Data Protection Act (2018)
- General Data Protection Regulation (2016/679)
- Freedom of Information Act (2000)

### RELATED POLICIES & DOCUMENTS

- Records Management Policy
- Records Retention Schedule
- Information Security Policy

# Data Protection Policy

## Contents

Data Protection Policy .....	2
1. Introduction and Purpose.....	2
2. Who does this policy apply to? .....	3
3. What is personal data? .....	3
4. Data Controller .....	3
5. Data Protection Officer (DPO) .....	4
6. Tasks of the DPO .....	4
7. Information Commissioner’s Office (ICO).....	4
8. Senior Information Risk Owner (SIRO) .....	5
9. GDPR Steering Group (SG) .....	5
10. Data Protection Advisers Group (DPAG) .....	5
11. Information Asset Owners (IAOs) .....	6
12. Roles and Responsibilities.....	6
13. Training .....	6
14. The Data Protection Principles .....	7
15. How does the University comply with the Principles? .....	7
16. The Rights of Individuals .....	8
17. Right of Access (Subject Access Requests) .....	9
18. Personal Data Breaches .....	9
19. Security .....	10
20. Accountability and Governance .....	10
21. Freedom of Information Act 2000 (FOIA) .....	11
22. Further Information and Assistance.....	11

## 1. Introduction and Purpose

Liverpool John Moores University (LJMU) collects, stores and processes a wide range of data about individuals during the course of its day-to-day business, and the use of personal data is an integral aspect of many of the University’s activities.

This Policy outlines how we comply with the data protection obligations as set out in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (together referred to as the “DP Legislation”) and how the University seeks to protect personal information relating to its staff, students, and other stakeholders.

The Policy is also to ensure that staff, students and those who use or have access to, or custody of personal data held by the University understand and comply with the rules governing the processing of personal information which they may have access to during their period of employment and/or studies.

Processing means the “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available ... or combination, restriction, erasure or destruction...”

The purpose of the DP Legislation is to protect the rights and privacy of individuals (referred to as ‘Data Subjects’) and to ensure that personal data is processed fairly, lawfully and transparently in compliance with the Data Protection Principles set out below at section 14.

The DP Legislation applies to all personal data processed by the University, or on behalf of the University, irrespective of where the data is held or in what format the data is held including paper, electronic and audio.

## **2. Who does this policy apply to?**

This policy applies to all staff, students and others who use or have access to, or custody of, personal data which is in the control of the University.

All staff are responsible for ensuring the security of the personal data that they use or have access to as part of their role.

It is a condition of employment that employees will abide by the rules and policies of the University. Any failure to do so may result in disciplinary proceedings.

## **3. What is personal data?**

Under the DP Legislation personal data means “any information relating to an identified or identifiable living person”.

Certain information referred to as ‘Special Categories Data’ is given more protection under the DP Legislation. Special Categories Data means “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership....genetic data, biometric data...data concerning health or data concerning a natural person’s sex life or sexual orientation”.

## **4. Data Controller**

LJMU is a registered Data Controller with the Information Commissioner’s Office (ICO) under registration number Z5616967.

## **5. Data Protection Officer (DPO)**

The University has a Data Protection Officer who provides advice and guidance on data protection matters to the University.

The Data Protection Officer is located within Legal and Governance Services and reports directly to the Vice Chancellor and the Board of Governors.

The University's Data Protection Officer can be contacted by email at: [DPO@ljmu.ac.uk](mailto:DPO@ljmu.ac.uk) or by phone on 0151 904 6134

We have published contact details of the DPO and communicated them to the ICO.

The DPO reports directly to our highest level of management and is given the required independence to perform their tasks.

We involve our DPO, in a timely manner, in all issues relating to the protection of personal data.

The DPO is sufficiently well resourced to be able to perform their tasks.

We do not penalise the DPO for performing their duties.

We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

## **6. Tasks of the DPO**

DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.

We will take account of our DPO's advice and the information they provide on our data protection obligations.

When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.

Our DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.

When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

## **7. Information Commissioner's Office (ICO)**

The Information Commissioner is an independent official appointment by the Government to uphold information rights in the public interest.

The ICO cover the requirements of the Data Protection Act, the General Data Protection Regulation, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations amongst other relevant pieces of legislation.

Further details about the work of the ICO and how to contact them can be found at [www.ico.org.uk](http://www.ico.org.uk)

## **8. Senior Information Risk Owner (SIRO)**

The Vice Chancellor is the University's SIRO and is responsible for the assurance of information security at LJMU and for championing compliance with the DP Legislation at the highest level.

## **9. GDPR Steering Group (SG)**

The SG was set up to provide strategic oversight for implementing and adhering to the University's obligations under the DP Legislation.

Members are senior representatives from across the whole of LJMU including Directors of Professional Services and Heads of Operations for the Faculties.

The SG promotes best practice across the organisation and members are accountable for ensuring GDPR compliance within their specific parts of the University with regard to achieving and remaining compliant.

The Terms of Reference for the SG can be found [here](#):

A list of the SG Members can be found [here](#):

## **10. Data Protection Advisers Group (DPAG)**

Each member of the SG has nominated a representative from their respective areas to join the Data Protection Advisers Group (DPAG).

The DPAG will help promote good practice and ensure that staff in their nominated areas are aware of LJMU data protection and information policies and processed.

The DPAG will assist the SG in achieving and maintaining compliance with the DP Legislation.

Members will be the first point of contact for assisting staff in resolving data protection queries at a local level and are responsible for disseminating key communications in relation to data protection.

The Terms of Reference for the DPAG can be found [here](#):

A list of DPAG Members can be found [here](#):

## **11. Information Asset Owners (IAOs)**

IAOs are the individuals across the University who are currently responsible for the main information systems and information assets.

Their role is to understand what information is held, what is added and what is removed, how information is moved and who has access and why.

They are able to understand and address risks to the information, know the vulnerabilities of the systems the data is stored in and ensure that information is processed in compliance with the DP legislation.

## **12. Roles and Responsibilities**

As well as the formal roles outlined above, all staff are responsible for the personal data that they process and have a duty to comply with the Data Protection Principles (set out below at section 14).

It is a condition of employment that all staff abide by the rules and policies of the University. Failure to do so may result in disciplinary proceedings.

Individuals who do not handle Personal Data as part of their normal work have a responsibility to ensure that any Personal Data they see or hear goes no further, e.g. data learned from a telephone call, contained on a computer print-out, or read on a computer screen.

LJMU staff will pay particular attention to the enhanced requirements for the processing of Special Categories Data.

## **13. Training**

The University aims to ensure that all staff are fully aware of their obligations under the DP Legislation and are aware of their personal obligations.

This is done by having data protection as a standing item on team meetings, a suite of policies and procedures to inform and guide staff as well as corporate communications to ensure a current awareness and consistency of message across the institution.

The University aims to provide staff with adequate training in relation to their data protection responsibilities.

All those who use or have access to or custody of personal data held by the University must complete the GDPR online training module on an annual basis.

Completion rates of the training will be reported regularly to the SG and DPAG and to Employment Committee as a standing agenda item and annually to the Board of Governors Audit Committee for oversight and monitoring.

Failure to complete the training module may result in disciplinary action and/or loss of access to University systems.

## 14. The Data Protection Principles

The Data Protection Principles ('the Principles'), as set out in the GDPR, provide a framework for processing personal data.

The Principles state that personal data shall be:

(a)	processed <b>lawfully, fairly</b> and in a <b>transparent</b> manner.
(b)	collected for <b>specified, explicit</b> and <b>legitimate</b> purposes only, and <b>not</b> in a way that is <b>incompatible</b> with those purposes.
(c)	<b>adequate, relevant</b> and <b>limited</b> to what is necessary in relation to the purposes for which they are processed (data minimisation).
(d)	<b>accurate</b> , and where necessary, <b>kept up to date</b> . Every reasonable step must be taken to ensure that inaccurate personal data are deleted or corrected without delay.
(e)	kept in a form which permits identification for <b>no longer than necessary</b> for the purpose(s) for which the information is processed.
(f)	processed in a manner that ensures appropriate <b>security</b> of personal data, including protection against unlawful processing, and accidental loss, destruction or damage.

LJMU must be able to demonstrate compliance with each of the Principles. The Principles are regarded as the minimum standards of practice for any organisation processing personal data.

More information about the Principles can be found on the ICO website [here](#).

## 15. How does the University comply with the Principles?

The University monitors and reviews its processing activities to ensure they are compliant with the DP Legislation.

The University only processes personal data for the specific purposes which have been communicated to Data Subjects via its Privacy Notices which explain how the University processes their personal data.

The University takes reasonable steps to ensure that the personal data it holds is accurate and kept up to date and to amend inaccurate or out of date personal data.

The University only holds the minimum amount of personal data necessary to enable it to perform its functions.

The University has an established Records Retention Schedule which is available within the Policy Centre and which all staff are required to abide by. Personal data will be erased once the need to hold it has passed in line with the Records Retention Schedule.

The University only uses data processors that provide sufficient guarantees of their technical and organisational measures for data protection compliance. Third parties with whom the University shares personal data or who process personal data on behalf of the University are expected to enter into formal agreements or contractual obligations which incorporate the requirements of the DP Legislation.

The University considers data protection and privacy issues upfront in everything that it does to ensure that it complies with the Principles. It considers data protection issues as part of the design and implementation of systems, services and business practices.

The University will undertake a Data Protection Impact Assessment, if appropriate, to identify and assess the impact on Data Subject's privacy as a result of amended or new means of processing personal data. This will be carried out in accordance with the Data Protection Impact Assessment Policy and procedure.

The University complies with the DP Legislation to allow Data Subjects to exercise their rights.

## **16. The Rights of Individuals**

The legislation provides the following rights for individuals:

- To be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.

These rights do not apply in all circumstances.

Further detailed guidance on the [Rights of Individuals](#) can be found on the ICO website.

The University's commitment to the Right of Access is explained in more detail below.

### **17. Right of Access (Subject Access Requests)**

The purpose of the right of access is to allow individuals to obtain a copy of their own personal data as well as other supplementary information. It helps individuals understand how and why the University is using their data, to check that it is accurate and that the University is processing the data lawfully.

Individuals can make a Subject Access Request verbally or in writing to the DPO.

LJMU is required to respond within one month of receipt of the request. However if the request is complex the response time may be extended by a further two calendar months starting from the day after receipt.

All staff must forward requests received under the right of access to the DPO without delay, noting the date of when the request was received. The date of receipt, anywhere in the University, determines the statutory deadline date that the University must respond by.

The University has processes in place to ensure that it responds to a subject access request without undue delay and within the statutory timescales. The [Data Subject Rights Policy](#) explains the procedure to be followed in the event of a request and can be found here.

### **18. Personal Data Breaches**

The University takes every step to prevent data breaches occurring but recognises that incidents may happen as a result of human error, system faults/failures or, in very exceptional circumstances, malicious activity. The University manages data breaches or suspected data breaches swiftly to minimise the associated risks to Data Subjects.

The University aims to ensure that staff know how and when to report any actual or suspected personal data breach and that any breach is handled correctly, lawfully and in a timely manner.

It has a Personal Data Breach Policy which explains the procedure to be followed in the event of a breach.

The DPO is responsible for the management of data breaches and for the provision of advice and guidance.

All breaches must be reported to the DPO as soon as the breach is discovered and in any event within 24 hours so that the DPO can assess whether a breach is reportable to the ICO/Data Subject(s).

A personal data breach can be reported to the DPO by using the online form which can be found here. [Breach Form](#)

## **19. Security**

The University is committed to ensuring the security of personal data and has appropriate physical, technical and organisational measures in place including for example swipe card access to buildings and offices and password protected access to our networks and systems.

LJMU staff who process personal data must ensure that it is kept secure at all times.

The University has various policies and procedures relating to the security of data held electronically and all staff must ensure that they understand and abide by these. A copy of the [Information Security Policy](#) can be found within the Policy Centre.

Care must be taken to ensure that PC's and other devices which are used to view personal data are not visible to unauthorised persons, and particular attention must be taken in public spaces. Screens should not be left unattended and staff should use the facility "lock" on their PC as appropriate.

In the case of manual data, files containing personal data must be kept securely in locked storage cabinets when not in use. Procedures should be in place to ensure that the movement of files can be tracked. Files must not be left on desks overnight or during periods when offices or work spaces are unattended.

The University provides facilities for the confidential destruction of paper documents containing personal data and staff must ensure that they dispose of personal data using these facilities.

The University has set up a Systems Data Working Group to look at a technical solution for records storage, retention and disposal. The aim is to align as fully as possible the data records, storage and retention rates within LJMU's corporate information systems to enable the University to operate as efficiently and compliantly as possible with the DP Legislation.

The University processes CCTV footage in accordance with relevant legislation and [code of practice](#) and provides appropriate privacy notices where necessary. The University's CCTV Systems Code of Practice is available to view within the Policy Centre.

## **20. Accountability and Governance**

The DPO retains the right to conduct audits and spot checks in relation to the processing of personal data and the University will hold staff to account for non-compliance with the Data Protection Principles and the Data Protection Policy.

The DPO, in addition to providing advice and guidance to the University will provide the following reports highlighting the University's compliance with DP Legislation

Annual Report to ELT and the Board of Governors (Audit Committee)

## **21. Freedom of Information Act 2000 (FOIA)**

The Freedom of Information Act 2000 does not give individuals an automatic right of access to personal data which is not their own. Any such requests will be considered by the DPO, and any decision relating to disclosure or non-disclosure of personal data must be made in accordance with the FOIA.

## **22. Further Information and Assistance**

The University has in place a number of policies and procedures to ensure that it complies with its duties under GDPR and to assist staff in understanding how data protection can impact on their day to day role. These can be found on the Policy Centre.

If you have any queries regarding data protection in your role or personal data breaches in your area, then please contact your Steering Group/DPAG representatives in the first instance.

The University's Data Protection Officer is available to advise further with regard to personal data breaches and this procedure generally and can be contacted at [DPO@ljmu.ac.uk](mailto:DPO@ljmu.ac.uk) or by phone on 0151 904 6134.

LJMU staff should not seek external legal advice or data protection advice from any other source without first consulting the Director of Legal & Governance Services and the Data Protection Officer.