Data Protection Policy

Responsibility for Policy:	University Secretary and General Counsel
Relevant to:	All Staff, Governors, sub contractor's apprentices, work placements and interns, Students and Academic Partnerships
Approved by:	ELT, 5th September 2019
Responsibility for Document Review:	Data Protection Officer
Date introduced:	2005
Date(s) modified:	April 2008, December 2008, September 2010, July 2013, May 2014, January 2015, January 2016, August 2016, September 2017, September 2018, September 2019, September 2020, September 2021
Next Review Date:	September 2022

RELEVANT DOCUMENTS

- Data Protection Act (2018)
- UK General Data Protection Regulation
- Freedom of Information Act (2000)

RELATED POLICIES & DOCUMENTS

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

Data Protection Policy

Contents

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 UK 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 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 and take account of the advice of our DPO.

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

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 DPO regularly reports to the SG on personal data breaches and training compliance. The SG monitor and analyse trends at a local level.

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.

SG members are responsible for keeping LJMU's Record of Processing Activities (ROPA) accurate and up-to-date for all processing within the area they represent. Guidance and procedure for LJMU's ROPA can be found on the DPO intranet page.

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 at an operational level 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 provides staff with adequate training in relation to their data protection responsibilities.

The university has a mandatory training programme which is signed off and endorsed by senior management. All those who use or have access to or custody of personal data held by the university must complete the Privacy and Security online training module on a quarterly basis. The content of the training programme is determined by the Information Security Manager and the Data Protection Officer to ensure it is appropriate and up to date.

Completion rates of the training will be reported regularly to the SG and DPAG as a standing agenda item and annually to the Board of Governors Audit & Risk 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 **lawfully, fairly** and in a **transparent** manner.
(b)	collected for **specified, explicit** and **legitimate** purposes only, and **not** in a way that is **incompatible** with those purposes.
(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 inaccurate personal data are deleted or corrected without delay.
(e)	kept in a form which permits identification for **no longer than necessary** for the purpose(s) for which the information is processed.
(f)	processed in a manner that ensures appropriate **security** of personal data, including protection against unlawful processing, and accidental loss, destruction or damage.

LJMU must be able to demonstrate compliance which 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 follows the advice of the DPO and takes account of their knowledge regarding data protection obligations.

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 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 complies with the DP Legislation to allow Data Subjects to exercise their rights. It provides guidance to staff on how to recognise data rights requests and the process to follow on receipt.

The university affords extra protection to Special Categories and Criminal Convictions data and to data of those individuals in vulnerable groups.

Principle a) - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

- LJMU will ensure that personal data is only processed where a lawful basis applies and where processing is otherwise lawful. The specific lawful basis for all processing will be recorded in the Record of Processing Activities (ROPA).
- Only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
- Ensure that data subjects receive full privacy information so that any processing of personal data is transparent. All processing will be explained in privacy notices, targeted at and appropriate for different groups of data subjects, which will usually be made available on our website.
- 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.

Principle b) - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the purposes.

- LJMU will only collect personal data for specified, explicit and legitimate purposes and will inform data subjects what those purposes are in a privacy notice.
- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If personal data is used for a new purpose that is compatible we will inform the data subject first.

Principle c) - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- LJMU will only collect the minimum personal data that is needed for the purposes for which it is collected.
- Ensure that the data it collects is adequate and relevant. All personal data held by LJMU will be linked to a recorded processing activity in the ROPA.

Principle d) - Personal data shall be accurate and where necessary, kept up to date.

- LJMU will ensure that personal data is accurate and kept up to date where necessary. Particular care will be taken where the use of the personal data has significant impact on individuals.

Principle e) - Personal data shall be 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.

- LJMU will only keep personal data in identifiable form for as long as is necessary for the purposes for which it was collected or where we have a legal obligation to do so.
- Once we no longer need the data it shall be deleted or rendered permanently anonymous. Retention limits are set out in our Records Retention Schedule which all staff must abide by.

Principle f) - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage, using the appropriate technical or organisational measures.

- LJMU will ensure that there are appropriate technical or organisational measures in place to protect personal data. Please see Chapter 20 for more details.

Accountability - The data controller shall be responsible for and be able to demonstrate compliance with these principles. **principle**

- LJMU will ensure that records are kept of all personal data processing activities and these are provided to the Information Commissioner on request.

LJMU will always have an appointed Data Protection Officer, please see Chapter 5 for more details.

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. Processing Special Category and Criminal Conviction Data

Schedule 1 Part 4 of the DPA 2018 requires that where LJMU processes "Special Category" or "Criminal Convictions" data, it is able to demonstrate compliance with the principles of the GDPR, as set out at Chapter 15 of this policy.

Special Category Data is defined in Article 9 of the GDPR and is outlined at 3 above. Criminal Conviction data is a defined widely by the ICO as encompassing

- Convictions
- Criminal activity;
- Allegations;
- Investigations; and
- Proceedings.

LJMU collects Special Category and Criminal Convictions data for a number of specific reasons as part of the administration of our organisation.

Where processing is based on the Article 9 conditions relating to (b) employment, social security and social protection, (h) health or social care, (i) public health or (j) archiving, research and statistics, LJMU must also satisfy an associated condition set out in Part 1 of Schedule 1 of the DPA 2018.

Where we are relying on reasons of substantial public interest, we must also meet one of the specific public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

Specific instances where Special Category and/or Criminal Convictions data is processed by LJMU are recorded in our ROPA.

19. 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. The DPO will assess the risk to data subjects on a case by case basis.

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

20. 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 identity of an individual must be verified, particularly over the telephone, before disclosing any personal data. Processes for verifying identification will vary locally depending on the service and staff must follow the process in their area.

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 LJMUs 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.

21. 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 will monitor and analyse trends in personal data breaches and data subject rights requests to understand themes and issues. Outputs will be reported to the SG and included in an Annual Report to ELT and the Board of Governors (Audit & Risk Committee).

22. 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.

23. 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.

Staff can report and escalate any data protection and information governance concerns directly to the DPO.

The DPO is available to advise further with regard to personal data breaches and this procedure generally and can be contacted at 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.