Data Protection Policy

Responsibility for Policy:	University Secretary
Relevant to:	All Staff, Students and Academic Partnerships
Approved by:	SMT in September 2018
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
Next Review Date:	September 2019

RELEVANT DOCUMENTS

- Data Protection Act (2018)
- General Data Protection Regulation (2018)
- Freedom of Information Act (2000)
- In the picture: A data protection code of practice for surveillance cameras and personal information [ICO]

RELATED POLICIES & DOCUMENTS

- Records Management Policy
- Records Retention Schedule
- Information Security Policy
- CCTV Systems Code of Practice

Data Protection Policy

1. Purpose and Status of the Data Protection Policy

1.1. 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.

1.2. This Policy outlines how we comply with data protection obligations as set out in the Data Protection Act 2018 (The Act) and the General Data Protection Regulation (GDPR) and how the University seeks to protect personal information relating to its staff, students, and other stakeholders. Its purpose is also to ensure that staff and students understand and comply with the rules governing the collection, use, retention and deletion of personal information, which they may have access to during their period of employment and/or studies.

1.3. The purpose of The Act and GDPR is to protect the rights and privacy of individuals, and to ensure that personal data is processed in compliance with the data protection principles as listed within the GDPR (see section 6).

1.4. The Act and GDPR applies to all personal data processed by the University, or on behalf of the University, irrespective of where the data is held and in what format the data is held.

1.5. It is a condition of employment that employees will abide by the rules and policies of the University. Compliance with The Act and GDPR is the responsibility of all members of the University. Any failure to abide by the Data Protection Policy may result in disciplinary proceedings.

2. Data Controller and the Data Protection Officer

2.1. LJMU is a registered Data Controller with the Information Commissioner's Office (ICO), under registration number Z5616769. In some limited cases, it is also a Data Processor of personal data.

2.2. The University has a named Data Protection Officer who provides advice and guidance on data protection matters to the University and its stakeholders. The Data Protection Officer is located within Legal and Governance Services and reports directly to the Board of Governors on the performance of this role. The University's Data Protection Officer is currently David Bridge.

3. Information Commissioner's Office (ICO)

3.1. 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.

3.2. Further details about the work of the ICO and how to contact them can be found at www.ico.org.uk

4. Contracts

4.1. All contracts that relate to the provision of goods and/or services that require the processing of personal data must include reference to the relevant data protection legislation and include the compulsory details and terms referenced on the ICO website contracts checklist and should be reviewed by the Data Protection Officer.

4.2. All data sharing agreements must be drafted with reference to the Data Protection Policy and in conjunction with the Data Protection Officer who is responsible for signing off all data sharing protocols. The ICO Data Sharing Code of Practice 2011 is in the process of consultation prior to being updated.

4.3. Any contracts relating to the sharing and/or processing of any personal data need to be approved by the University's Legal team before the data is shared or processed. The Legal team will work in conjunction with the Data Protection Officer to ensure that the appropriate contractual documents are put in place to protect both the University and the data subject.

4.4. Further details relating to contracts can be found in the Policy Centre including *Contracts and Liabilities Between Controllers and Processors* and *Controller and Processor Contracts Checklist*.

5. Data Protection Advisers Group (DPAG)

5.1. All academic and professional service areas of the University are required to nominate a Data Protection Adviser, to join the Data Protection Advisers Group (DPAG). The DPAG, chaired by the Data Protection Officer, is tasked with providing local advice to staff and students; contributing to institutional and local policies and procedures; and disseminating key communications in relation to data protection. Further details relating to the Data Protection Advisers Group can be obtained from the secretariat@ljmu.ac.uk.

6. The Data Protection Officer (DPO)

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

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

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

6.4 We do not penalise the DPO for performing their duties.

6.5 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.

7 Tasks of the DPO

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

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

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

7.4 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.

7.5 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.

8 Roles and Responsibilities

8.1 All LJMU staff members have a duty to comply with the Data Protection Principles, as listed below.

8.2 All LJMU staff will take responsibility for complying with the LJMU Data Protection Policy, and implementing any working practices with a Privacy by Design approach.

8.3 LJMU staff will ensure that the University has a lawful basis for processing personal data and will ensure that subjects are notified as appropriate (see Privacy Notices: Staff Guidance in the LJMU Policy Centre).

8.4 LJMU staff will pay particular attention to enhanced requirements for the processing of Special Category Data (Sensitive Personal Data).

8.5 All LJMU staff will complete the Data Protection Online Module on an annual basis.

8.6 All LJMU staff will ensure compliance with the University's Information Security Policy.

9 Data Protection Principles

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

9.2 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.

9.3 LJMU must be able to demonstrate compliance which each of the Principles by clearly documenting its processes and, where appropriate, the use of Privacy Statements which inform individuals as to why, what purpose and on what the legal basis data is collected and how they can access the data. A guide to Privacy Statements: Staff Guidance is available within LJMU Policy Centre.

10 Lawful Basis for Processing Personal Information

10.1 In order to comply with Principle (a), the University must ensure that it has identified, and communicated where appropriate, at least one of the following lawful conditions for processing personal data.

Article 6(1)	Conditions for Processing Any Personal Data
(1)	The data subject has given consent.[1]
(2)	It is necessary for the performance of a contract, or the data subject has taken steps to enter into a contract.
(3)	It is necessary due to a legal obligation.
(4)	It is necessary to protect the vital interests of the subject or a third party.
(5)	It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.
(6)	It is necessary for the legitimate interests of the Controller or a third party.

10.2 For special category personal data (sensitive personal data), at least one of the following conditions must also be met:

Article 9(2)	Article 9 Special Category Data
(1)	The data subject has given explicit consent.[1]
(2)	It is necessary for the purposes of employment, social security and social protection law.
(3)	It is necessary to protect the vital interests of the subject or a third party.
(4)	The processing is carried out by a not-for-profit body.
(5)	The processing relates to personal data which are manifestly made public by the data subject.
(6)	It is necessary for legal claims.
(7)	Is it necessary for reasons of substantial public interest.
(8)	It is necessary for the purposes of medicine, the provision of health or social care or treatment, or the management of health or social care systems and services.
(9)	It is necessary for public health.
(10)	It is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

[1] *Consent is defined as freely given, specific, informed and unambiguous indication of the data subject's wishes. Clear affirmative action is required. Without this consent is not valid. However Consent is just one of the conditions and it may not be the most appropriate condition.*

11 The Rights of Individuals

11.1 The legislation provides the following rights for individuals:

11.1.1 To be informed;
11.1.2 The right of access;
11.1.3 The right to rectification;
11.1.4 The right to erasure;
11.1.5 The right to restrict processing;
11.1.6 The right to data portability;
11.1.7 The right to object; and
11.1.8 Rights in relation to automated decision making and profiling.

11.2 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 below.

12 Right of Access (Subject Access Requests)

12.1 The purpose of the Right of Access is to allow individuals to obtain a copy of their own personal data, confirm the accuracy of personal data and check the lawfulness of processing to allow individuals to exercise the right of objection or correction, if necessary.

12.2 Individuals can exercise their Right of Access in writing to the Data Protection Officer, providing direction as to the information they are seeking and proof of identification. All requests received via a third party must be supported by the appropriate level of consent. LJMU will also require evidence of your identity to verify that you are the data subject and have the right to request such data.

12.3 LJMU is required to respond within one month of receipt of the request. However if the request is complex or you make more than one request, LJMU response time may be a maximum of three calendar months, starting from the day after receipt.

12.4 The requested information will be provided in permanent form, in either hard copy format or electronic format. The University will discuss the preference of format and delivery with the Subject.

12.5 Some information may be exempt from the Right of Access, or the University may be able to consider the request to be manifestly unfounded or excessive. The Data Protection Officer must be consulted when considering an exemption.

12.6 All staff must forward requests received under the Right of Access to the Data Protection Officer 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.

13 Exemptions

13.1 There are a number of exemptions that the University can rely on to either disclose or withhold personal data in particular circumstances without breaching the Data Protection Principles. The application of an exemption is the decision of the Data Protection Officer.

14 Data Breaches

14.1 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.

14.2 The University has a statutory responsibility to report breaches to the Information Commissioner's Office without undue delay and, within 72 hours of becoming aware of it if it is likely to result in a risk to the rights and freedoms of individuals. It will also notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and if notification is required by law.

14.3 The University's Data Protection Officer is responsible for the management of data breaches and for the provision of advice and guidance. To comply with

this deadline 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. The Data Protection Officer will decide whether a breach meets the reporting requirement.

15 Security

15.1 LJMU staff responsible for processing personal data must ensure that it is kept securely and in compliance with Principle (f), *"processed in a manner that ensures appropriate security of personal data, including protection against unlawful processing, and accidental loss, destruction or damage."*

15.2 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.

15.3 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.

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

15.5 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.

15.6 The University provides facilities for the confidential destruction of paper documents.

16 Retention of Personal Data

16.1 The University has an established Records Retention Schedule (RRS), which is available within the Policy Centre, and which all staff are required to abide by. Indeed, compliance with the RRS will assist staff and students to comply with data protection legislation.

16.2 The University and its staff will comply with Principle (e*),* personal data will be *"kept in a form which permits identification for no longer than necessary for the purpose(s) for which the information is processed."*

17 Training

17.1 The University will provide all staff with adequate training in relation to their data protection responsibilities.

17.2 All staff, including sessional and contractors, are required to complete the Data Protection Online Module on an annual basis. Failure to complete the Module may result in disciplinary action and/or loss of access to University systems.

17.3 Completion rates will be reported to the University's Data Protection Advisers Group as a standing item and annually to the Board of Governors Audit Committee for oversight.

18 Privacy by Design and Data Protection Impact Assessments

18.1 LJMU will take a Data Protection by Design approach to the processing of personal data and the systems used.

18.2 The University will conduct a Data Protection Impact Assessment for projects or activities that may have a negative impact on the privacy of individuals.

18.3 A Data Protection Impact Assessment, is similar to a risk assessment, whereby risks to privacy are identified and solutions embedded to mitigate or minimise the risks.

18.4 Further details in relation to Privacy by Design and Data Protection Impact Assessments can be found within the LJMU Policy Centre Privacy Impact Assessment Guidance, and on the ICO website, Privacy Impact Assessment Template, Privacy Impact Assessment: Initial Risk Assessment Template.

19 Accountability and Governance

19.1 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.

19.2 The Data Protection Officer, in addition to providing advice and guidance to staff, student and other stakeholders, will provide the following reports highlighting the University's compliance with The Act and the GDPR:

19.2.1 Annual Report to the Board of Governors;
19.2.2 Annual Report to the Board of Governors Audit Committee;
19.2.3 Annual Report to the Strategic Management Team;
19.2.4 Monthly performance indicators to the Strategic Management Team; and
19.2.5 Any other ad hoc reports, as necessary.

19.3 The Data Protection Officer will maintain and monitor the following registers, and will make them available to the Information Commissioner upon request:

19.3.1 Personal Information Register (coded against the Records Retention Schedule);
19.3.2 Data Breach Register;
19.3.3 Privacy Notice Register;
19.3.4 Right of Access (Request) Register; and
19.3.5 Data Protection Impact Assessment Register.

20 Freedom of Information Act 2000 (FOIA)

20.1 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 Data Protection Officer, and any decision relating to disclosure or non-disclosure of personal data must be made in accordance with the FOIA.

21 Further Guidance and Resources

21.1 Further advice and guidance is available within the LJMU Policy Centre, and on the ICO website. In addition, staff and students can contact their local DPAG member or the University's Data Protection Officer for guidance.

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

21.3 Staff must consult all relevant policies and guidance documents within the Policy Centre when processing personal data including codes of practice.

22 Contact Details

22.1 Data Protection Officer DPO-LJMU@ljmu.ac.uk