Data Protection Act 1998 Policy

Responsibility for Policy:	University Secretary
Relevant to:	All Staff, Students and Academic Partnerships
Approved by:	SMT in September 2016
Responsibility for Document Review:	Manager, Secretariat (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
Next Review Date:	January 2018

RELEVANT DOCUMENTS

- Data Protection Act (1998)
- 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

- LJMU Publication Scheme
- Records Management Policy
- Records Retention Schedule
- Personal Development & Performance Review Policy

1. INTRODUCTION

1.1 Liverpool John Moores University (LJMU) is committed to full compliance with the Data Protection Act 1998 ["the Act"] and the incoming General Data Protection Regulation (GDPR) which will come into effect on 25th May 2018, and recognises in full the rights and obligations established by the Act and regulations in relation to the management and processing of personal data. This Policy is intended to serve as general guidance for staff and students in implementing the letter and spirit of the provisions and principles of the Act. More detailed guidance is available on the data protection pages of the website at:
https://www2.ljmu.ac.uk/secretariat/68133.htm

2. DATA PROTECTION ADVICE

2.1 The Data Protection Officer for LJMU provides general advice on data protection and freedom of information. The Data Protection Officer should be informed of all data subject requests received by LJMU staff or students, i.e. requests from staff or students for personal information about themselves.

2.2 Guidelines and good practice notes on compliance with the Act can be found within the staff Policy Centre.

3. A BROAD OVERVIEW OF THE ACT

3.1 The purpose of the Data Protection Act and the GDPR is to protect the rights and privacy of individuals, and to ensure that data about them is not processed without their knowledge and is processed with their consent wherever possible.

4. DEFINITIONS

4.1 **Personal Data**
Data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (the University), and includes any expression of opinion about the individual and any indication of the intentions of the University or any other person in respect of the individual.

4.2 **Sensitive Personal Data**
Personal data consisting of information as to –

(a) the racial or ethnic origin of the data subject,

(b) his/her political opinions,

(c) his/her religious beliefs or other beliefs of a similar nature,

(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992) http://www.legislation.gov.uk/ukpga/1992/52/contents

(e) his/her physical or mental health or condition,

(f) his/her sexual life,

(g) the commission or alleged commission by him/her of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

4.3 **Data Controller**

A person who (either alone or in common with other persons) or organisation who determines the purposes for which and the manner in which any personal data, are, or are to be, processed. LJMU is the data controller. The data controller must be a "person" recognised in law, that is to say:

- individuals;
- organisations; and
- other corporate and unincorporated bodies of persons.

4.4 **Data Processor**

Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

4.5 **Processing**

In relation to processing personal information or data this means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

4.6 **Data Subject**

A living individual who is the subject of the personal data

4.7 **Third Party**

Any person other than –

(a) the data subject,

(b) the data controller, or

(c) any data processor or other person authorised to process data for the data controller or processor.

5. NOTIFICATION

5.1 The Act requires all data controllers to inform the Office of the Information Commissioner of:

(a) the purpose for which personal data is held or used, e.g. student administration, research, marketing.

(b) the types of person for whom personal data is held, e.g. students, employees etc. and the class of data e.g. personal identifiers, education records etc.

(c) the source or sources from which the data is obtained and the persons to whom the data may be disclosed.

(d) the countries to which data is transferred.

6. THE DATA PROTECTION PRINCIPLES

6.1 Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

(1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met http://www.legislation.gov.uk/ukpga/1998/29/schedule/2, and

(b) In the case of sensitive personal data, at least one of the conditions of Schedule 3 is also met http://www.legislation.gov.uk/ukpga/1998/29/schedule/3

(2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

(3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

(4) Personal data shall be accurate and, where necessary, kept up to date.

(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

(6) Personal data shall be processed in accordance with the right of data subjects under this Act.

(7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

(8) Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7. HANDLING PERSONAL DATA FAIRLY AND LAWFULLY

7.1 In order for personal data to be processed fairly and lawfully you must –

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

7.2 LJMU staff must ensure that consent is always obtained. The most usual methods are by ensuring that there is a data protection statement, (known as a Privacy Notice) included on all forms capturing personal data, within guidance notes for the completion of forms, in relevant staff and student handbooks, and on any forms completed on-line. The guidance on consent has been updated to ensure it complies with the GDPR. This is held within the Policy Centre.

Guidance on data privacy notices is available within the Policy Centre

8. RIGHT OF SUBJECT ACCESS

8.1 This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, an individual who makes a written request and pays a fee (£10) is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;

- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

8.2 Guidance on how to access your personal data is held on the website htttp://www.ljmu.ac.uk/about-us/data-protection

8.3 LJMU must ensure that it has proof of the identity of the requester to prevent any unlawful disclosure.

8.4 A data subject can request access to their personal data through another party such as a lawyer or an advocate. A signed letter or form of authority from the data subject must be provided before any data is disclosed.

8.5 LJMU is required by the Act to respond within 40 calendar days of receipt of the request and the fee, but every effort should be made to respond as quickly as possible. The 40 days applies to all requests for personal data, whether routine or complex. Please note that the new GDPR, which will come into effect on 25th May 2018, provides for a 20 day response with no charge.

8.6 If the request arises as part of another matter, for instance, an 'Extenuating Circumstances' request; an academic appeal; complaint; grievance; or disciplinary matter; the requirements of the DPA must not be overlooked, particularly the 40 day deadline. In these circumstances, staff must seek advice from the Data Protection Officer.

8.7 Some information **may be exempted from the Subject Access Requirements**, **for example information held in confidence, or legal professional privilege**. The Data Protection Officer will apply such exemptions in consultation with the Legal Department. The University's Legal Department will make it clear on any correspondence or guidance they provide to staff that information is bound by legal professional privilege and this information should not be shared with anyone other than expressly agreed by the Legal Department. The University's Data Protection Officer will have access to such information to ensure the correct exemption is applied.

8.8 The requested data should normally be provided in permanent form on paper, including e-mail.

8.9 If the data subject believes that their personal data is inaccurate; out-of-date; held unnecessarily; or is offensive; they have the right to have the information rectified; blocked; erased; or destroyed. The data subject also has the right to insist that the University ceases to process their personal data if such processing is causing or is likely to cause unwarranted substantial damage or substantial stress to them or to another. The data subject may also have a right to compensation if it can be proven that damage or distress has been caused.

Please contact the Data Protection Officer if you need further advice or guidance.

9. FREEDOM OF INFORMATION ACT 2000 (FOIA)

9.1 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 request must be considered and any decision to refuse disclosure must be made in accordance with the FOIA. The University's Manager, Secretariat is also the University's Data Protection Officer and Freedom of Information Officer for LJMU and is a source of guidance for the FOIA.

9.2 Any request from a data subject for their own personal data made under the FOIA is dealt with under the Data Protection Act.

10. THIRD PARTY DATA AND THE SUJBECT ACCESS RIGHT

10.1. When handling a subject access request, sometimes another individual (known as a third party) may be identified in the personal data to be disclosed. The University will only disclose third party data under the Act with the consent of that third party, or if it is reasonable to do so without consent. In determining if whether it would be reasonable, LJMU must balance its duty of confidentiality to the third party against the rights of the data subject; consider any steps taken to seek consent; whether the third party is capable of giving consent; or any express refusal of consent by the third party. These considerations are made by the Manager, Secretariat (Data Protection Officer).

11. EXEMPTIONS

11.1 There are number of exemptions from the provisions of the Act. These allow the University to either disclose or withhold data from disclosure in particular circumstances, without breaching the data protection principles. Any exemptions are applied by the Data Protection Officer.

11.2 Guidance on the exemptions and their application can be obtained from the Data Protection Officer.

12. GENERAL RESPONSIBILITIES OF LJMU STAFF

12.1 When processing personal data, LJMU staff must ensure that they abide by the Data Protection Act 1998, and from 25th May 2018 the General Data Protection Regulation, and process data in accordance with the eight data protection principles. All University business conducted by email should be held on University provided systems and email accounts to ensure the security and confidentiality of University business and to ensure the University can comply with a person's right to access any records it holds.

12.2 All new projects or policies (including software/technical programmes) containing or collecting personal information are subject to a Privacy Impact Assessment (PIA). This is usually the responsibility of the Project Manager or Policy author. All PIAs should be recorded by the Data Protection Officer.

Please see guidance and templates for conducting Privacy Impact Assessments within the Policy Centre.

12.3 If in any doubt, staff should refer to this policy, any other guidance provided on the University's website, the Data Protection Officer, or the Director of Legal and Governance Services.

12.4 All staff are required to complete the mandatory e-learning module on an annual basis which gives assurance to the Information Commissioner that all University staff receive training around data protection. The module will be updated to ensure compliance with GDPR.

12.5 If you have found that a data protection or data security breach has occurred please inform the Data Protection Officer. For further information on how to report a breach and what types of situations could constitute a data breach please see the section on 'Data Security Breaches' and 'Data Security Breach Management' within the Policy Centre.

12.6 Please ensure you do not share information that is held in confidence or is bound by legal professional privilege. **See 8.7 above.**

13. SECURITY OF DATA

13.1 LJMU staff responsible for processing personal data must ensure that it is kept securely to avoid unauthorised access and only disclose to those authorised to receive it.

13.2 The University has policies and procedures in regard to the security of electronically held data and staff must ensure that they read and understand these policies and procedures. A copy of the Information Security Policy can be found in the Staff Policy Centre. All staff and students are required, when they first log onto the University's network, to confirm their understanding and acceptance of the Computing Regulations and Conditions of Use: https://www2.ljmu.ac.uk/itservices/128759.htm and on an annual basis thereafter.

13.3 Care must be taken to ensure that PCs and terminals on which personal data is viewed are not visible to unauthorised persons, especially in public places. This will also include information held on mobile devices. Screens showing personal data should not be left unattended. Staff should use the facility "lock computer" on their PC if they are absent from their desk for a short period of time, and should "log-off" for longer periods.

13.4 The University processes CCTV footage in accordance with 'In the picture: A data protection code of practice for surveillance cameras and personal information', published by the Information Commission's Office in May 2015. The University's CCTV Systems Code of Practice and the Code of Practice on the Use of Cameras in Teaching/Learning Environments are available in the University's Staff Policy Centre.

13.5 In the case of manual data, files containing personal data should be kept in locked storage cabinets when not in use. Procedures for booking files in and out should be used so that their movements can be tracked. Files should not be left on desks overnight.

13.6 The University provides facilities for the confidential destruction of paper documents. Details of this service and related guidance are available at: https://www2.ljmu.ac.uk/secretariat/96882.htm

14. EXTERNAL [LEGAL] ADVICE

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

15. THE ROLE OF THE INFORMATION COMMISSIONER

15.1 The Information Commissioner is an independent official appointed by the Government to oversee the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. The Commissioner reports annually to Parliament. The Commissioner's decisions are subject to the supervision of the Courts and the Information Tribunal.

15.2 The mission of the Office of the Information Commissioner is to promote public access to official information and to protect personal information.

15.3 The Information Commissioner provides good practice guidance and interpretation of the Act for data controllers and advice to the public on how to access personal data. The website of the Office of the Information Commissioner is: http://www.ico.org.uk/

15.4 The Commissioner has formal powers to force a data controller to take or refrain from certain actions if he has determined there has been, or is likely to be, a breach of the Act. Failure to comply with a Decision Notice or an Enforcement Notice may be dealt with as though the University had committed contempt of court. As from April 2010, the Information Commissioner (ICO) has been able to impose fines of up to £500,000 as a penalty for serious breaches of the Act.

16. MONITORING

16.1 For monitoring purposes, the Secretariat maintains a record of all requests for information.

16.2 LJMU will provide an annual report on the University's compliance with information legislation to the Strategic Management Team and Audit Committee. Monthly performance indicators are also interrogated by the Strategic Management Team.

16.3 This policy will be reviewed biennially or in light of any new legislative changes.

17. PROVISION OF GUIDANCE

Data Protection Officer
0151 231 3116, Secretariat@ljmu.ac.uk