

University of London

Data Protection Policy

Contents

1. Policy statement	3
2. Scope.....	3
3. Definitions.....	3
4. Principles.....	4
5. Legal basis for processing – personal data	4
6. Legal basis for processing – special category data	5
7. Rights.....	6
8. Data Protection by design.....	7
9. Security	7
10. The Data Protection Officer	7
11. Training and awareness	7
12. Using data processors	8
13. Academic Research	8
14. The University as Processor	8
15. Further Information	9
16. Version control.....	9

1. Policy statement

The University is committed to complying with the General Data Protection Regulation as an academic institution, an employer and as a service provider. In order to do this the University commits that:

- We process our data fairly and legally
- We support the rights of individuals
- We keep our personal data secure
- We design privacy into our systems and processes

2. Scope

The University is subject to the General Data Protection Regulation and associated data protection legislation. The University is required to register as a Data Controller with the Information Commissioner's Office. The University's notification (registration number: Z5419651) covers the University's central academic activities, administrative functions, libraries and business services, including its wholly-owned companies. The University is an exempt charity and a 'public authority' according to the definitions of the regulation.

3. Definitions

The General Data Protection Regulation governs the processing of personal data. The following definitions are used:

- **Personal data** are data which can identify living individuals. As well as images, names and contact details it can also include numerical or statistical information from which an individual's identity can be derived.
- **Special Category Data** are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- A **Data Subject** is the individual who is the subject of personal data.
- A **Data Controller** determines the purposes for which personal data are processed. The controller is ultimately responsible for the personal data, whether they pass the data to a data processor or not. This includes the responsibilities of responding to Subject Access Requests and complaints from data subjects.
- A **Data Processor** is any individual or organisation who processes personal data on behalf of – and according to the purposes defined by – the data controller.

4. Principles

The University is required to process personal data according to the following six principles:

Data Protection Principles	The context for the University
<i>Lawfulness, fairness and transparency</i>	The University explains to its staff, students and customers how it processes personal data at the point of collection and for what purposes
<i>Purpose limitation</i>	The University only uses the personal data it has for the purposes it was collected for
<i>Data Minimisation</i>	The University only collects personal data which is relevant to the purposes it is required for
<i>Accuracy</i>	The University ensures that the data is correct, up to date and able to be rectify any mistakes quickly
<i>Storage Limitation</i>	The University does not retain personal data for longer than it is needed
<i>Integrity and Confidentiality</i>	The University protects its personal data against unauthorised access, loss or destruction by a range of security measures

5. Legal basis for processing – personal data

The University needs to meet one of the six lawful bases in order to process personal data. The most common for the University will be the following:

Legal basis	Examples for the University
<i>Necessary for the performance of a contract</i>	Covers the majority of processing for our students and staff
<i>Data subject has given consent to the processing</i>	Covers mailing lists, marketing and other optional services for staff, students and customers
<i>Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</i>	Covers the retention of our student pass lists and transcript information for awards and verification
<i>Necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data</i>	Covers activities around alumni, charitable works and marketing of commercial services

6. Legal basis for processing – special category data

For special category data, in addition to a lawful basis listed in Section 5, University is required to have an additional legal basis for processing, as set out in Article 9 of the Regulation.

Legal basis	Examples for the University
<i>processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law</i>	Sickness absence, Notifying the University of Trade Union membership
<i>processing relates to personal data which are manifestly made public by the data subject;</i>	Alumni research, honorary degrees, ethical donations assessment
<i>processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee,</i>	Occupational therapy assessments
<i>processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes</i>	Analysis and reporting of equality and diversity information

The legal basis for processing will be listed in the University's Record of Processing Activities, produced in line with Article 30 of the Regulation.

7. Rights

Data subjects – our students, staff and customers – have a number of rights under the Regulation. These include:

Right	The context for the University
<i>Right of access</i>	Data subjects have the right to find out about what we are doing with their data, check we're holding it correctly and to obtain a copy of what we hold.
<i>Right to rectification</i>	The University makes every effort to ensure its data is accurate. If a data subject thinks something we hold about them is wrong, they can ask for this to be corrected. The University will assess the request and correct any inaccuracy.
<i>Right to erasure / right to be forgotten</i>	Data subjects have the right to ask us to remove or delete data we hold on them. The University will assess the request against the criteria in Article 17 and respond accordingly.
<i>Right to restriction of processing</i>	Data subjects may, in the course of a dispute with the University about the use of their data, ask the University to stop using their data if certain criteria applies.
<i>Right to data portability</i>	Data subjects have the right to ask the University to provide them with a re-usable electronic copy of their data to allow them to transfer it to another provider. This only covers data submitted to the University by the subject or data observed from the subject's use of a service. If technically possible, the University will consider transferring information directly to another provider.
<i>Right to object</i>	Data subjects have the right to object to processing based on legitimate interests, legal obligation or for the purposes of direct marketing or for "scientific or historical research purposes or statistical purposes". The University will assess the request and respond accordingly.
<i>Automated decision making, including profiling</i>	If the University is making decisions about data subjects through purely automated means, such as a computer algorithm, data subjects can appeal against this decision. The University will ensure that subjects can express their point of view and have member of staff provide a review and explanation of the decision.

Forms and guidance for making a rights request are available on the data protection pages on the University's website.

8. Data Protection by design

The University is committed to ensuring privacy is built into its processes and outcomes. New projects involving personal data are required to carry out a privacy impact assessment to identify privacy risks and plan appropriate mitigation.

9. Security

The University's overarching ICT security policy and programme supports compliance around the 'integrity and confidentiality' principle of the regulation in ensuring appropriate technical measures are in place to protect personal data. Details of the security policy can be found on the University's website. There is a personal data breach notification procedure in place in accordance with Article 33 of the Regulation.

10. The Data Protection Officer

In accordance with Article 37-39 of the Regulation the University has appointed a data protection officer, whose contact details are as follows:

Data Protection & Information Compliance Manager

University of London

Senate House

Malet Street

London WC1E 7HU

data.protection@london.ac.uk

11. Training and awareness

The University is committed to ensuring its staff have the requisite training and awareness around data protection. All staff must undertake the compulsory 'Data Protection' and 'IT Security' training. Further resources and training are provided on the staff intranet and on request from the Data Protection & Information Compliance Manager. As referenced in the staff terms and conditions, breach of data protection law due to unauthorised access, misuse or loss may result in disciplinary action, up to and including dismissal.

12. Using data processors

The University may use an external contractor or 'data processor' to store or manage its data. It will process this data only for purposes specified by the University and will be bound by contract to meeting the University's obligations under the General Data Protection Regulation. Where data is passed outside the EEA, the University will take the relevant steps to ensure there is adequate protection in place.

13. Academic Research

Academic research which involves the processing of personal data is subject to the General Data Protection Regulation. All academic projects are subject to the Research Ethics policy, which includes specific directions for projects involving personal data.

14. The University as Processor

Where the University, in the course of its academic or commercial activities, acts as a processor it is subject to the requirements of Article 28 of the Regulation and will:

- process the personal data only on documented instructions from the controller
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- take all measures required pursuant to Article 32 'Security of processing'
- not engage another processor without prior specific or general written authorisation of the controller
- assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights
- make available to the controller all information necessary to demonstrate compliance

15. Further Information

Any questions relating to the Data Protection Act or this policy should be directed to the Data Protection & Information Compliance Manager at: data.protection@london.ac.uk.

16. Version control

Date	Version	Reason for change	Author
January 2018	0.1	Initial draft	Data Protection & Information Compliance Manager
May 2018	0.2	Updated with comments from consultation	Data Protection & Information Compliance Manager
May 2018	1.0	Approved by Information Technology and Governance Group (ITGG)	Data Protection & Information Compliance Manager