Data Protection Policy

1. Introduction

1.1. London Metropolitan University is required by law to conform to the principles of the General Data Protection Regulations (GDPR). This policy is a statement of the measures which the University has adopted to ensure it is able to comply with the requirements of the Regulations. The University undertakes to apply the policy to all persons associated with the University. In this context, 'all persons associated with the University' encompasses all Governors, staff, students, and any person acting as a data processor on behalf of the University.

1.2. The University holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes. When handling such information, the University, and all staff or others who process or use any personal information on behalf of the University must comply with the principles relating to the processing of personal data as set out in the GDPR.

1.3. Definitions

Personal Data

Data is information about a living person which identifies and relates to that person, such as a name, identification number - including location data and online identifiers. Personal data may be of a sensitive nature, for instance, information about a person's health or ethnicity (see 'Special Categories of Personal Data'). Personal data may be held in any format including paper or digital. Anything that can identify a living person is covered and must be treated in accordance with the requirements of the Regulations.

Data Controller

The individual/organisation registered which determines the purpose for which, and the manner in which any personal data is processed, and who is responsible for ensuring the requirements of GDPR are complied with. For this institution, 'London Metropolitan University' is the Data Controller.

Data Subject

A living individual who is the subject of personal data: e.g. Governors, staff, current and prospective students, graduates, former students, suppliers of

goods and services, business associates, etc.

Data Processor

This includes any person who processes personal data on behalf of the data controller. Employees of the University are excluded from this definition but it could include suppliers which handle personal data on behalf of the University. The University is responsible for the processing of personal data on its behalf by data processors, and must enter into agreements with data processors which meet the requirements of GDPR.

Data Users

This includes all employees, and occasionally some students, whose work involves using personal data for which the University is responsible. Data users have a duty to protect the information they handle by following the University's data protection and security policies.

Processing

Obtaining, recording or holding data, accessing, altering, adding to, deleting, changing, disclosing or merging personal data and anything else which can be done with personal data. Processing also includes transferring personal data to third parties.

Special Categories of Personal Data

A type of personal data recognised by the Act, consisting of information covering one or more of the following categories:

- The racial or ethnic origin of an individual
- Political opinions
- Religious beliefs
- Membership of a trade union
- Physical or mental health
- Sexual orientation
- Biometric data
- Genetic data

2. The Data Protection Principles

2.1. Management of personal data at the University will comply with the six data protection principles set out in GDPR. These are as follows:

a) Personal data shall be processed fairly, lawfully and in a transparent manner.

b) Personal data shall be obtained for a specified, explicit and legitimate purpose and shall not be processed in any manner incompatible with that purpose.

c) Personal data shall be adequate, relevant and limited to what is necessary for the purpose or purposes for which they are processed.

d) Personal data shall be accurate and, where necessary, up-to- date. Reasonable steps must be taken to ensure personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.

e) Kept in a form that permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed. Personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

f) Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Lawful basis for processing

3.1. The processing of students personal data is necessary for the performance of a task in the public interest (Art.6(1)(e) and for the purpose of the legitimate interests pursued by the university . As a higher education institution (HEI) the university's public task is teaching and research. Details of how the university handles student personal data can be found in the Student Privacy Notice - http://www.londonmet.ac.uk/media/london-metropolitan-university/london-met-documents/professional-service-departments/university-secretarys-office/compliance/data-protection/Student-Data-Protection-Statement.pdf

3.2. The processing of staff personal data is necessary for the performance of a contract (Art.6(1)(b) and compliance with a legal obligation (Art.1(1)(c). Details of how the university handles staff personal data can be found in the Staff Privacy Notice -

4. Processing of Special Categories of Personal Data

4.1. The University may process special category personal data for its business purposes. Such information may be required for some jobs and/or courses, in particular where the University has a duty under the relevant legislation to ensure that staff are suitable for the job, and students for the courses offered. The University may also require such information for other legitimate purposes e.g. the administration of policies relating to sick pay, staff absence or equal opportunities, or for academic assessment.

4.2. Stricter conditions apply to the processing of special categories of personal data. Where such data is being processed not only must the data controller meet the requirements of the Principles and the conditions set out in Article 6 of the Regulations, but processing is prohibited unless at least one of the

conditions in Article 9 can also be satisfied.

4.3. Agreement to the University processing specified classes of personal data is a condition of acceptance of a student on to any course, and a condition of employment for staff.

5. Staff Responsibilities

5.1. All staff shall

- Ensure that any information they provide to the University in connection with their employment is accurate and up-to-date;
- Inform the University of any errors or changes to information which they have provided (e.g. change of address);
- Check the information the University makes available from time to time and, where appropriate, follow procedures for updating entries on University databases;
- Correctly process data during the course of their employment;
- Comply at all times with the university's policies regarding data security, network security, remote and home working, and network access;
- Comply with the University's requirements regarding the ethical approval of research (including any conditions attached to ethical approval), where personal data is processed in the course of a research project;
- Ensure that personal data for which they are responsible is kept secure and is accurate and up to date;
- Promptly report any breaches of the Data Protection Policy (including unauthorised disclosure, loss or destruction of personal data) to the Data Protection Officer (see Further information, below).

6. Student Responsibilities

6.1. All Students shall

- Ensure that any information they provide to the University in connection with their studies is accurate and up-to-date;
- Inform the University of any errors or changes to information which they have provided (e.g. change of address);
- Comply with the University's requirements regarding the ethical approval of research (including any conditions attached to ethical approval), where personal data is processed in the course of a research project;
- Check the information the University makes available from time to time and, where appropriate, follow procedures for updating entries on University databases.

6.2. Students in a position where they are processing personal data about staff or other students (e.g. as a student representative on a University committee or working in a temporary role while studying), must ensure that they comply with

University policies and with the requirements of the Regulations. Where a student processes personal data as an employee, they are subject to the dutiesapplicable to staff outlined above and the requirements of their employment contract.

7. Security

7.1. It is of the utmost importance that data is kept securely and precautions must be taken against physical loss or damage to data. This applies equally to data processed off-site (e.g. by staff working remotely or at home), as to data processed on London Met premises. In fact, off-site processing presents a potentially greater risk of accidental loss, theft or damage to data.

7.2. All staff should ensure that any personal data which they hold is kept securely, and that personal information is not disclosed either orally or in writing or accidently or otherwise to any unauthorised third party.

7.3. It is essential to protect the security and confidentiality of data during storage, transportation, handling and destruction. GDPR requires data controllers to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

7.4. All personal information in the form of hard copy records, when not in use should be

- Kept securely
- Files should be put away in secure storage at the end of the working day, and should not be left on desks overnight.

7.5. Electronic personal data should be

- Password protected, with passwords being changed regularly so that only authorised people can view or alter confidential data.
- Encrypted, where necessarily held for University purposes on mobile devices (e.g. laptops, USB sticks).

7.6. Staff should be aware of and ensure that they comply at all times with the

- Acceptable Use Policy
- Home PC and Laptop Policy
- Information Protection (Security) Policy
- Password Policy and Guidelines
- Remote Access Policy

7.7. Care must be taken to ensure that PCs and terminals on which personal data are processed are not visible to unauthorised persons, especially in public places. Screens on which personal data are displayed should not be left unattended.

8. Vendors, Contractors and Suppliers

8.1. Vendors, contractors and suppliers are often required to have access to areas in which personal data may be stored or processed. It is therefore necessary to ensure contractors are:

- Controlled, documented and wearing some form of identification;
- Restricted from unnecessary admittance to areas where personal data is held or processed;
- Required to sign non-disclosure agreements where access to personal data is unavoidable;
- Party to an agreement with the University to comply with the University's Data Protection policies and procedures.

8.2. Where an organisation processes personal data on the University's behalf (e.g. under an outsourcing arrangement), the organisation is a data processor and the University (as the data controller) must ensure that the requirements of the GDPR are met. The Regulations requires the University to enter into a written contract with the data processor which must require the data processor to have data security arrangements in place which meet the requirements of the Regulations. Staff should contact the University Secretary's Office for advice before entering into data processor arrangements (see Further information, below).

9. Right to Access Personal Data

9.1. Staff and students have the right under GDPR to access personal data which is kept about them in both computer and hard copy files. Any person wishing to exercise this right (Subject Access Request) should do so by submitting their request in writing to the University's Information Compliance Officer[2]. Any member of staff who receives a written request directly should forward the request to the Information Compliance Officer. Staff and students must not respond to Subject Access Requests themselves.

9.2. When making such a request, the individual must provide a suitable means of identification. This must be a certified copy of your passport or driving licence.

9.3. The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month as required by the Regulations unless the request is complex or numerous. In such instances, the reason for the delay will be explained in writing by the Information Compliance Officer to the individual making the request.

9.4. Staff are required to assist the Information Compliance Officer in meeting the University's obligation to comply with Data Subject Access Requests, and must provide all relevant information when requested to do so.

[2] See the university's page on subject access requests for guidance: http://www.londonmet.ac.uk/about/policies/data-protection/subject-access-requests/

10. Disclosing Personal Data

10.1. Personal data should not be disclosed to third parties without the permission of the individual concerned. In this context "third parties" include family members, friends, and government and other public bodies unless disclosure is exempted by the Regulations or required by other legislation.

10.2. Under certain circumstances, data may however be released to third parties:

- For the purpose of protecting the 'vital interests' of the individual (this means where the individual's life is at risk)
- For the prevention or detection of crime
- For the apprehension or prosecution of offenders
- For the discharge of regulatory functions, including securing the health, safety and welfare of persons at work
- Where the disclosure is required by legislation, by any rule of law or by the order of the court
- Where there is a legitimate interest in the release of the information which is not overridden by prejudice to the rights, freedoms or legitimate interests of the individual who is the subject of the data.

If in doubt, contact the University's Information Compliance Officer (see Further information, below).

11. Direct Marketing

11.1. The use of personal data in direct marketing is subject to the Regulations and to the requirements of the Privacy and Electronic Communications Regulations (which apply to electronic marketing, including phone, fax, email or text). 'Direct marketing' does not apply to communications which the University sends to students in the normal course of administering the relationship with them, e.g. regarding their programme of study or events at London Met.

11.2. Personal data should not be processed for the purposes of direct marketing without the consent of the individual concerned. Individuals have the right to prevent their personal data from being used for direct marketing and the University will cease using a data subject's personal data for marketing purposes when requested to do so.

12. Disposing of Personal Data

12.1. The Regulations places an obligation on the University to ensure that personal data is disposed of securely. All staff have a responsibility to consider safety and security aspects when disposing of personal data in the course of their work. Staff should ensure that:

- All paper or microfilm documentation containing personal data is permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.
- USB sticks, CDs and other removable media should be physically destroyed when they are no longer required.
- When vacating a building or moving offices, staff should ensure that they check all filing cabinets, cupboards, shelves and pedestals for any personal data.

13. Retention of Data

13.1. The University will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements. To this end, the University will maintain a Records Retention Schedule in order to help avoid excessive retention or premature destruction of personal information. Information about recommended retention periods can be found in our retention schedule -,

14. Compliance

14.1. Compliance with the Regulations is the responsibility of all students and staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings.

15. Further information

15.1. Any questions or concerns about the interpretation or operation of this policy should be referred to the Data Protection Officer (see below). Further guidance and advice on Data Protection is available on university webpages: http://www.londonmet.ac.uk/about/policies/data-protection/

Contact

Dr Christopher Ince
Data Protection Officer
Tel: 020 7133 2004
Email: c.ince@londonmet.ac.uk

Tracy Brathwaite
Information Compliance Officer
Tel: 020 7133 4137
Email: t.brathwaite@londonmet.ac.uk

Version control information:

Document last reviewed by: Information Compliance Officer/University Secretary
Next review: October 2018
Approved by: Senior Management Team, April 2018