



Data Protection Policy (including Schedules 2 & 3)

INTRODUCTION

Policy Statement

London Metropolitan University is required by law to conform to the principles of the Data Protection Act (1998). 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 DPA (1998).

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, accredited visitors and any person acting as a data processor on behalf of the University. Any breach of the Data Protection Policy or the DPA (1998) will automatically be considered a breach of discipline and existing London Metropolitan disciplinary proceedings will apply.

Data Protection Terms

Data

"Data is information about a living person which identifies that person, and which may be of a sensitive nature, for instance, their health, ethnicity or marital status. This includes opinions about that person, and the intentions of other people towards them. The Act covers a wide range of formats: Paper files; electronic files and databases; WebPages; Photographs; Publications; Voice recordings; CCTV; X-rays. Anything that can identify a living person, and this includes where they were at a specific time, is covered and must be treated in accordance with the requirements of the Act".

Data Controller

The individual/organisation registered with the Information Commissioner who is responsible for ensuring the requirements of the Data Protection Act (1998) are complied with. For this institution, 'London Metropolitan University' is the Data Controller.

Data Subject

An individual, who is the subject of personal data, this will include governors, staff, current and prospective students, graduates, former students, suppliers of goods and services, business associates, etc.

Personal Data

Information that identifies and relates to a living individual, this includes any expression of opinion or intention about the individual.

Processing

Accessing, altering, adding to, deleting, changing, disclosing or merging data and anything else which can be done with data.

Relevant Filing System

Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible: i.e. structured by reference to individuals (e.g. alphabetical), by reference to criteria relating to individuals, by numerical reference (e.g. student number) etc.

The Data Protection Principles:

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, and
 - (b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
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 were 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 rights 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 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.

In addition Schedule 2 states that processing may only be carried out where one of the following conditions has been satisfied i.e. where;

- The individual has given his/her consent to the processing
- The processing is necessary for the performance of a contract with the individual
- The processing is required under a legal obligation
- The processing is necessary to protect the vital interests of the individual
- The processing is necessary to carry out public functions
- The processing is necessary in order to pursue the legitimate interests of the data controller or certain third parties (unless prejudicial to the interests of the individual).

Freedom of Information Act (2000)

This act creates new rights of access to information held by public bodies in England, Wales and Northern Ireland. Further education institutions and organisations fall within the remit of the Act. The F.O.I Act (2000) requires institutions to respond to requests within 20 days, in conjunction with the Data Protection Act (1989) it is apparent how important an effective Records Management Programme is, in information retrieval, and this is something we are working towards. Further guidance will be forthcoming.

Sensitive Data

Stricter conditions apply to the processing of sensitive data. This category includes information relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. Where such data is being processed not only must the controller meet the requirements of the Principles and Schedule 2, but processing is prohibited unless at least one of the conditions in Schedule 3 can be satisfied.

The explicit consent of the individual will have to be obtained before sensitive data can be processed unless the controller can show that the processing is necessary based on one of the criteria laid out in Schedule 3 of the Act.

Notification

The University is registered as a Data Controller and a Data Processor and has notified the Information Commissioner of:

1. The personal data that it will process
2. The categories of data subjects to which personal data relates
3. The purposes for which the personal data will be processed.

The information currently held by the University and the purposes for which it is processed form the official notification that has been submitted to the Information Commissioner's Office. If processing for a new or different purpose is introduced the individuals affected by that change will be informed and the official notification will duly be updated to reflect the said change.

Responsibilities of Staff and Students

Staff are responsible for:

- Ensuring that any information they provide to the University in connection with their employment is accurate and up-to-date
- Informing the University of any errors or changes to information which they have provided (e.g., change of address)
- Checking the information the University sends out from time to time giving details of information kept and processed about staff
- Correct processing of data during the course of their employment.

Students must likewise ensure that any information they provide to the University is: accurate and is kept up-to-date.

If students find themselves 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 whilst studying), they must ensure that they comply with the University Policy and with the requirements of the Act.

Security

- It is of the utmost importance that data is kept securely
- Precautions must be taken against physical loss or damage, to data
- 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 accidentally or otherwise to any unauthorised third party
- It is essential to protect the security and confidentiality of data during storage, transportation, handling and destruction.

All personal information in the form of manual records should be:

- Kept in a locked filing cabinet: or
- kept in a locked drawer, in a lockable room.

If information is computerised, it should be:

- Password protected, with passwords being changed regularly so that only authorised people can view or alter confidential data; or
- kept only on disk, which should be kept securely in a lockable desk or cabinet to avoid physical loss or damage.

Vendors, Contractors, and Suppliers

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 are wearing some form of identification
- Restricted from unnecessary admittance to areas where personal data is held or processed

- Required to sign nondisclosure agreements where access to personal data is unavoidable

Data Subject Rights and Access to Personal Data

Staff and students have the right to access information, which is kept about them in both computer and manually held files. Any person wishing to exercise this right should make their request in writing to the University's Data Protection Officer. When making such a request, referred to as a Subject Access Request the individual must:

- Provide a suitable means of identification
- Inform the Data Protection Officer where they believe the information is held.

The Data Protection Act (1998) stipulates that the University may charge £10.00 for this provision and that the information must be provided within 40 days. The University does not have to divulge information, which identifies another person, unless that person consents to this.

Data Subjects further rights

The University undertakes to:

- Ensure that no decisions that affect them are based solely upon an automated decision-taking process
- Prevent processing likely to cause damage or distress
- Prevent processing for the purposes of direct marketing
- Act to rectify, block, erase or destroy inaccurate data
- Ask the Information Commissioner to assess whether any part of the (1998) Act has been contravened.

Transitional Provisions

Transitional Provisions contained within the (1998) Act allows the University to claim an exemption from specified parts of the legislation for a particular period of time. The University can reserve the right to apply the following transitional relief, to manual data only, during the period 24th October 2001 to 23rd October 2007. This applies to manual data that was being held and processed immediately before 24 October 1998. Manual data added on or after 24 October 1998 will not qualify.

Qualifying data will be exempt from the following Data Protection Principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(c) at least one of the conditions in Schedule 2 is met, and

(d) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

However the University must still inform data subjects about the type of data they hold about them, how they intend to use it, to whom they are likely to disclose it too and how long they intend to retain it.

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 were 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. The provisions relating to rectification, blocking, erasure and destruction of inaccurate data.

Disclosing Personal Data

Personal data should not generally be disclosed to third parties without the permission of the individual concerned. In this context "third parties" includes family members, friends, local authorities, government bodies and the police, unless disclosure is exempted by the (1998) Act or by other legislation. Under certain circumstances, data may however be released. Note that among other circumstances the Act permits release of data without express consent:

- For the purpose of protecting the vital interests of the individual (e.g., release of medical data where failure to do so could result in harm to, or the death of, the individual)
- For the prevention of 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.

If in doubt contact the University's Data Protection Officer.

In the case of applicants from overseas information on the progress of an application may be sought on their behalf by a person resident in this country. Such information should not be released unless an authorisation has been confirmed. The Admissions office has produced a proforma for such cases.

Disposing of Personal Data

The Data Protection Act (1998) places an obligation on the University to err on the side of caution when disposing of personal data. All staff have a responsibility to consider safety and security aspects when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved (how sensitive is it?), and the format in which it is held. 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

Collection and Processing of Personal Data relating to Disability

The University will often collect student disability information at the admission stage (for example, through UCAS, and through interviews etc.) but collection of disability data may also occur throughout the period of study or employment. The University will provide:

- Mechanisms to ensure that where disability data is provided for a stated purpose, such as to ensure adequate service provision, it is not misused for other purposes, such as to make a decision about whether or not to admit a student to a course of study
- A system whereby when there is a need to disclose disability data to external organisations, prior consent of the data subject should be obtained for each disclosure. The data subject should be informed about the nature of the information to be disclosed, the intended recipient, and the purpose of disclosure should be given to the data subject.

CONTACT

Peter Fisher, Records & Compliance Officer

Tel: 020-7320-3001 (City Campus); 020-7133-2411 (North)

Email: p.fisher@londonmet.ac.uk

SCHEDULE 2:

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.
2. The processing is necessary -
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary -
 - (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under any enactment,
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
 - (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order-
 - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary-
 - (a) in order to protect the vital interests of the data subject or another person, in a case where-
 - (i) consent cannot be given by or on behalf of the data subject, or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
 - (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing-
 - (a) is carried out in the course of its legitimate activities by any body or association which-
 - (i) is not established or conducted for profit, and
 - (ii) exists for political, philosophical, religious or tradeunion purposes,
 - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing-

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by-

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) The processing-

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms

of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

Updated: 23rd January 2012