

Produced by Academic Registry

July 2012

General Policy Statement GPS4

Data Protection Policy

1. Middlesex University needs to keep certain information about its past, current and potential employees and students, and other users of Middlesex University facilities to allow it to function effectively, monitor performance and achievements. The University needs to process information so that it can recruit and pay staff, organise programmes and comply with legal obligations to funding bodies, government regulations and company legislation such as health and safety and equal opportunities. As a research institution, Middlesex University needs to keep information on individuals who are the subjects of research projects.

Middlesex University complies with the eight principles of the Data Protection Act 1998, that data is:

1. processed fairly and lawfully and shall not be processed unless certain conditions are met.
 2. obtained for specified and lawful purposes and not further processed in a manner incompatible with that purpose.
 3. adequate, relevant and not excessive.
 4. accurate and where necessary up to date.
 5. kept for no longer than necessary.
 6. processed in accordance with data subjects' rights.
 7. protected by appropriate security.
 8. not transferred without adequate protection.
2. Middlesex University staff and students or others who process or use any personal information must ensure that they follow these principles at all times.
 3. CDS is the nominated processor for all post, both internal and external, sent to and within the University. CDS opens the post (save those items on our Exception list) and scans it electronically to be emailed to the recipient, where it is treated in accordance with the principles set out in this policy document. Save for the process of opening the post and scanning it, there is no human intervention in the transmission of the data. CDS is obliged to comply with the Data Protection Act 1998 and the principles set out in this policy document. Any breach of the Data Protection policy or the 1998 Act by a University member, be they a member of staff or student, may result in disciplinary procedures being instigated against them and possibly a criminal prosecution.

4. The Data Protection Officer and the Departmental Coordinators

4.1 The University, as a body corporate, is the Data Controller under the Act, and the Board of Governors, as the governing body of the University, is ultimately responsible for compliance with the 1998 Act.

4.2 The Middlesex University Data Protection Officer, who is the named contact with the Data Protection Commissioner, is:

Teresa Kelly
0208 411 6018
t.kelly@mdx.ac.uk.

The Middlesex University Data Protection Officer will ensure that the Middlesex University data protection notification is kept up to date using information provided by the departmental Data Protection Coordinators.

4.3 Each School and Service will appoint a departmental Data Protection Coordinator. The Data Protection Coordinator will ensure that the personal data held by their department is kept securely and used properly, within the terms of the Act. They will be responsible for informing the Data Protection Officer of the types of personal data held in their department, and any changes or new holdings. The Data Protection Officer will inform the Data Protection Coordinators of any changes or amendments to the Act, and advise on the implementation of the 1998 Act.

5. Notification of Data Held and Processed

5.1 All staff, students, and other users are entitled to know:

- what personal information Middlesex University holds and processes about them and why.
- how to gain access to it.
- how to keep it up to date.
- what Middlesex University is doing to comply with its obligations under the 1998 Act.

5.2 The data types of student information held about past, present and future students may include:

- personal information
- sensitive personal data
- assessment information
- financial information

and is processed to comply with the requirements of official bodies eg. HEFCE, SLC, as part of the educational process. Notice of this will be given in the Student Guide and Regulations.

5.3 The data types of staff information held include:

- personal information
- sensitive personal data
- work performance information
- financial information

and is processed for the proper administration of the employment relationship both during and after employment.

5.4 The Data Protection Officer will, on receipt of a written request from an individual member of staff or student or other user, provide details of the information held about that individual and the reasons for which it is processed within the legal time requirement of 40 days from receipt of the written request. The request cannot be actioned unless the data subject provides adequate identification and adequate information to enable the University to find the relevant data entries.

6. **Staff Guidelines for Data Protection**

6.1 Staff should ensure that they are familiar with the Data Protection Policy. Compliance with the policy is the responsibility of all members of Middlesex University. Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken, or access to Middlesex University facilities being withdrawn, or even a criminal prosecution.

6.2 All staff are responsible for:

- Checking that any information that they provide in connection with their employment is accurate and up-to-date.
- Informing Human Resource Services of any changes to information, which they have provided. eg. changes of address.
- Informing Human Resource Services of any errors or changes.

6.3 Personal names, Middlesex University telephone numbers, and Email addresses of Middlesex University staff involved in the teaching and administration of collaborative programmes within the EU/EEA area will be shared with the relevant partner institutions on a need-to-know basis.¹

6.4 Personal names, Middlesex University telephone numbers, and Email addresses may be published on the University's internet facility, unless the individual concerned informs the Data Protection Officer, in writing, that they do not wish this information to be disseminated in this way. Those responsible for producing pages for the internet, whether for general University information or for specific Schools or Services, are responsible for ensuring that any individual named on that page has not refused permission to publish their name and Email address, by checking either with the individual or with the Data Protection Officer.

6.5 Staff whose work involves the management of student data must ensure they observe the eight data protection principles detailed in paragraph 1.

6.6 Staff whose work includes responsibility for supervision of students' academic work have a duty to ensure that students observe the eight data protection principles.

6.7 All staff should ensure that any holding or processing of personal data is included in the Middlesex University notification.

¹ The data will, therefore, be shared only within the EU (currently 27 countries), plus 3 EEA countries which have agreed to be bound by the EU Data Protection Directive (Norway, Liechtenstein, and Iceland) and also the following countries which have been judged by the EU to afford 'an adequate level of protection' of personal data (currently, Switzerland, Canada, Argentina, Guernsey, Jersey, Andorra, Faroe Islands, Israel and the Isle of Man).

7. Data Security

7.1 All staff are responsible for ensuring that:

Any personal data, which they hold, whether in electronic or paper format, is kept securely.

Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also be a criminal matter in which the individual concerned could be held individually criminally liable as well as the University.

7.2 Incoming and Internal Mail:

CDS is the nominated processor for all post, both internal and external, sent to and within the University. CDS opens the post (save those items on our Exception list) and scans it electronically to be emailed to the recipient, where it is treated in accordance with the principles set out in this policy document. Save for the process of opening the post and scanning it, there is no human intervention in the transmission of the data. CDS is obliged to comply with the Data Protection Act 1998 and the principles set out in this policy document.

Paper-based mail sent within or from outside the University which are marked 'Personal' or 'Private and Confidential', may also be opened by CDS and scanned accordingly.

Staff are discouraged from using their Middlesex University address for non-University matters.

8. Student Guidelines for Data Protection:

8.1 Students should ensure that they are familiar with the Data Protection Policy.

Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken, or access to Middlesex University facilities being withdrawn, or even a criminal prosecution.

8.2 The University processes data relating to its students for a variety of purposes. These include but are not limited to :-

Maintenance of the student record (including personal and academic details) and management of academic processes (for example, academic audits, examination boards and awarding of degrees).

The management of college residences.

Alumni operations, including fund-raising.

The provision of advice and support to students via, amongst others, the Academic Registry, Student Services (including counselling careers etc.), academic staff and the Disability Support Service.

Internal research, including monitoring quality and performance

The University, via Schools, Student Services, the Academic Registry, and other ancillary departments, allows access to employees and agents of the University (on a need-to-know basis only). Student information is disclosed to a variety of third parties or their agents, notably

Students' sponsors (including LEAs, the Student Loans Company and funding councils).

Relevant government departments to whom we have a statutory obligation to release information (including HEFCE, the Higher Education Statistics Agency, UKBA and Council Tax officers).

Current or potential employers of our students.

The JISC plagiarism detection service.

The agency compiling the National Student Survey.

Disclosures to organisations not listed above will be made in specific legitimate circumstances. Consent from the student will be sought where necessary and students will be informed of such disclosures unless exceptional circumstances apply.

8.3 Students are responsible for:

Ensuring that all personal data provided to Middlesex University is accurate and up to date.

Informing the relevant Student Office of any changes to information which they have provided. E.g. change of address.

Informing the University of any errors or changes

Students who, in the course of their programme of study, process personal data must do so in accordance with the provisions of the 1998 Act, the University's Data Protection policy and any amendments or supplementary guidance issued from time to time.

Students who are undertaking research projects using personal data must ensure that:

The research subject is informed of the nature of the research and consents to their personal information being used.

Their Supervisor is informed of the proposed research before it begins, and ensures that Middlesex University is licensed to undertake this kind of research.

All information is kept securely.

8.4 Assessment grades:

The University will publish assessment grades for each module, by student number, on campus notice boards and/or electronically. It will publish degree classifications alphabetically by student name on notice boards and as appropriate for the Awards Ceremony.

9. Subject Consent to Processing Personal Information

9.1 Middlesex University may ask for information about a student's or an employee's health for use in the event of a medical emergency. Middlesex University may also ask for information about an individual's criminal convictions, race and gender and marital status to ensure that Middlesex University is a safe place for everyone and to enable the University to operate policies like equal opportunities and to comply with legislation.

Middlesex University or its nominated document processor (CDS), processes personal/sensitive personal data with the consent of the individual.

Because some information is considered sensitive, all staff and students are required to give Consent to Process regarding particular types of information. Offers of

employment or programme places may be withdrawn if an individual refuses to consent to this, without good reason. The University also reserves the right to process data lawfully in accordance with the 1998 Act even where express consent has not been given.

10. Publication of Information relating to Staff and Students of the University

10.1 It is the policy of Middlesex University to make public as much information about the University as possible in any medium. This includes but is not limited to:

Organisational structure showing roles and names
Members of the Board of Governors of the University
Members of committees of the Board of Governors and Academic Board
List of key staff
Photographs of key staff
List of students to whom awards have been made or are likely to be made by the University.

Any individual having good reason for wishing details in these lists or categories to remain confidential should contact the Middlesex University Data Protection Officer.

Information that is already in the public domain is exempt from the 1998 Act.

10.2 In accordance with the Freedom of Information Act, the University has issued a Publication Scheme, and will make available on request University documents that give information about the structure, policies and operations of the University. Reports, minutes and other similar documents made available under the Scheme will be amended so that statements and contributions made by staff and students are not attributed to identified individuals.

Care must be taken when capturing close-up images (including photos, videos, film) of staff or students, whether or not these individuals are named. Of key importance is the expectation of privacy on the part of those whose image it is proposed to capture. Consent to image capture is not required in the public spaces of the University (including atrium, corridors, refectory or library) but is required where the expectation of privacy is greater (including classrooms, studios, labs, meeting rooms, accommodation blocks). See full 'Filming and Image Capture Guidelines' on the Data Protection section of Academic Registry Intranet site.

11. Rights to Access Information

11.1 Staff, students and other users of Middlesex University facilities have the right to access personal data that is being kept about them insofar as it falls within the scope of the 1998 Act. Any person who wishes to exercise this right should make their request in writing, to the Data Protection Officer. When making such a request, the individual must tell the Data Protection Officer where they believe this information is held. Middlesex University reserves the right to charge the recommended administrative fee on each occasion that access is requested, but will normally waive this right where the request is reasonable.

Middlesex University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the statutory 40 days.

12. **Retention of Data**

Middlesex University keeps some forms of information for longer than others, in line with Financial, Legal, or Archival requirements. The Data Protection Officer will advise on retention periods of different types of data.

13. **Research Purposes Exemption**

Data collected fairly and lawfully for the purpose of one piece of research can be used for other research, providing that the final results of the research do not identify the individual. Such data must not be processed to support measures or decisions with direct consequences for the individuals concerned, or in a way, which is likely to cause substantial damage or distress to any data subject. Records of questionnaires and contacts may be kept, in order that the data can be revisited and/or re-analysed. This exemption is only applicable to research, and cannot be used to provide information about a particular individual.

This policy will be reviewed in July 2016