

**Produced by Executive**

**November 2014**

**General Policy Statement GPS4**

**Data Protection Policy**

1. **Objectives of the policy**

To ensure that:

* Proper procedures are in place for the processing and management of personal data
* There is someone within the organisation who has specific responsibilities for data protection compliance.
* A supportive environment and culture of best practice processing of personal data is provided for staff
* All staff understand that their responsibilities when processing personal data and that methods of handling that information are clearly understood
* Individuals wishing to submit a subject access request are fully aware of how to do this and who to contact
* Staff understand that subject access requests need to be dealt with promptly and courteously
* Individuals are assured that their personal data is processed in accordance with the data protection principles, that their data is secure at all times and safe from unauthorised access, alteration, use or loss
* Other organisations with whom personal data needs to be shared or transferred, meets compliance requirements
* Any new systems being implemented are assessed on whether they will hold personal data, whether the system presents any risks, damage or impact to individuals’ data and that it meets this policy’s requirements

1. **The eight principles**

The Data Protection Act 1998 contains eight “Data Protection Principles”. These specify that personal data must be:

1. Processed fairly and lawfully
2. Obtained for specified and lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept any longer than necessary
6. Processed in accordance with the “data subject’s” (the individual’s) rights
7. Securely kept
8. Not transferred to any other country without adequate protection in situ
9. **Scope of policy**

* This policy has been written within relevant ICO guidelines.
* Definitions and terms used in relation to the Data Protection Act can be found at <http://ico.org.uk/for_organisations/data_protection/the_guide>
* This policy applies to all personal data and sensitive personal data collected and processed by Middlesex University in the conduct of its business, in electronic format in any medium and within structured paper filing systems.
* This policy applies to all University employees, whether permanent, temporary, contractors, or consultants.
* Disciplinary action may be taken against staff failing to comply with this policy.
* Middlesex University is the Data Controller of, and registered with the Information Commissioner’s Office (ICO) for collecting and using personal data. The registration reference is Z5439728**.**

1. **Policy Principles**

In order to meet the requirements of the 8 principles of the DPA, Middlesex University adheres to the following values when processing personal data:

***4.1 Fair Collection and Processing***

* The specific conditions contained in Schedules 2 and 3 of the DPA regarding the fair collection and use of personal data will be fully complied with.
* Individuals will be made aware that their information has been collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection.
* Personal data will be collected and processed only to the extent that it is needed to fulfil business needs or legal requirements.
* Personal data held will be kept up to date and accurate.
* Retention of personal data will be appraised and risk assessed to determine and meet business needs and legal requirements, with the appropriate retention schedules applied to that data.
* Personal data will be processed in accordance with the rights of the individuals about whom the personal data are held.
* Individuals whose personal information is held on a University database will be provided with the option to ‘opt out’ of receiving future communications.
* A ‘cease processing request’ from an individual will be acknowledged within 3 working days, with the final response within 21 days. The final response will state whether the University intends to comply with the request and to what extent, or will state the reasons why it is felt the requestor’s notice is unjustified.
* Staff will advise the Data Protection Officer in the event of any intended new purposes for processing personal data. The Data Protection Officer will then arrange for a Privacy Impact Assessment to be conducted.

***4.2 Security***

* Appropriate technical, organisational and administrative security measures to safeguard personal data will be in place.
* Staff will report any actual, near miss, or suspected data breaches to the Data Protection Officer for investigation. Lessons learnt during the investigation of breaches will be relayed to those processing information to enable necessary improvements to be made.
* Any unauthorised use of corporate email by staff, including sending of sensitive or personal data to unauthorised persons, or use that brings the University into disrepute will be regarded as a breach of this policy.
* Relevant Data Protection Awareness Training will be provided to staff to keep them better informed of relevant legislation and guidance regarding the processing of personal information. Data protection training will also promote awareness of the University’s data protection and information security policies, procedures and processes.

***4.3 Sharing and disclosure of personal information***

* The University shall routinely make certain personal information publicly available. Examples include publication of degree results in graduation booklets, contact details on the website etc. The University will undertake to cease such activity for any data subject on the grounds of such disclosure causing damage and distress on application to, and agreement by, the Data Protection Officer.
* Regular information sharing with third parties, where there is a valid business reason for sharing information, shall be carried out under a written agreement setting out the scope and limits of sharing. Data Processing Agreements will be applied to all contracts and management agreements where the University is the data controller contracting out services and processing of personal data to third parties (data processors). These agreements will clearly outline the roles and responsibilities of both the data controller and the data processor.
* All data processors shall agree to conform to this policy and the Act, and as far as possible, indemnify the University against any prosecution, claim, proceeding, action or payments of compensation or damages without limitation and provide any personal information specified on request to the Data Protection Officer.
* Where applicable the University will inform individuals of the identity of third parties to whom we may share, disclose or be required to pass on information to, whilst accounting for any exemptions which may apply under the Data Protection Act 1998 and other relevant legislation.
* Personal data will not be transferred outside the European Economic Area unless that country or territory can ensure a suitable level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

***4.4 Access***

* Members of staff will have access to personal data only where it is required as part of their functional remit.
* Staff are made aware that in the event of a Subject Access Request being received in Middlesex University, their emails may be searched and relevant content disclosed, whether marked as personal or not.
* A relevant contact address will be made available on the internet for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how Middlesex University is processing their data, or about our handling of their request for information
* A Subject Access Request will be acknowledged to the data subject within 3 working days, with the final response and disclosure of information (subject to exemptions) within 40 calendar days. A fee may be charged for this, at our discretion, which will be no more than £10.
* A data subject’s personal information will not be disclosed to them until their identity has been verified.
* Third party personal data will not be released by Middlesex University when responding to a Subject Access Request or Freedom of Information Request (unless consent is specifically obtained, obliged to be released by law, or necessary in the substantial public interest).
* All data subjects have a right of access to their own personal data. Advice will be provided to data subjects on how to request or access their personal data held by the University.

***4.5 Links with the Freedom of Information Act 2000***

* The Freedom of Information Act 2000 enables greater public access to information processed by public bodies such as Middlesex University. However, personal data continues to be protected by the Data Protection Act 1998, and is therefore exempt from disclosure under the Freedom of Information Act (Section 40).

1. **Data Protection responsibilities**

|  |  |
| --- | --- |
| **Who** | **What** |
| University as a corporate body | Data Controller |
| Board of Governors | Ultimately responsible for compliance with the 1998 Act |
| Data Protection Officer (Teresa Kelly) | Maintain the University notification with the ICO  Advise staff on data protection compliance  Coordinate responses for subject access requests  Report any personal data breaches to the ICO/police as appropriate  Issue data sharing guidance and oversee data sharing agreements between the University and third parties  Develop, administer, disseminate, review and support application of this policy |
| Executive Briefing Group members | Support the Data Protection Policy and application of it within respective Schools/ Services |
| Director of CCSS | Ensure adequate policies are in place for security of electronic information |
| CDS | Nominated processor for all post sent to and within the University  Compliance with the Data Protection Act 1998 and with the principles set out in this policy |
| Line managers | Support and encourage staff to comply with the Policy  Ensure that line reports do not have access to personal data if it is not required as part of their functional remit |
| All staff | Be familiar with and comply with the policy  Ensure that information provided in connection with employment is up-to-date and accurate  Observe and comply with the 8 data protection principles  Do not attempt to gain access to information that is not necessary to hold, know or process  Know and understand how to deal with subject access requests  Note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual and staff member |
| All students | Be familiar with and the policy and comply where necessary  Ensure that personal information provided is up-to-date and accurate  Observe and comply with the 8 data protection principles  Note that unauthorised disclosure of personal data will usually be a disciplinary matter. |

1. **Related policies and documents**

* Computer Use Policy for Staff - <http://www.intra.mdx.ac.uk/Assets/HRPS36.pdf>
* Records Management - [www.intra.mdx.ac.uk/working-here/policies/records-management/index.aspx](http://www.intra.mdx.ac.uk/working-here/policies/records-management/index.aspx)
* Freedom of information - <http://www.intra.mdx.ac.uk/Assets/GPS5.pdf>
* CCTV Policy - <http://www.intra.mdx.ac.uk/working-here/policies/security/index.aspx>
* Access Control - <http://www.intra.mdx.ac.uk/working-here/policies/security/index.aspx>
* Security Policy - <http://www.intra.mdx.ac.uk/working-here/policies/security/index.aspx>
* JANET acceptable Use Policy - <http://www.intra.mdx.ac.uk/working-here/policies/IT-policies/index.aspx>
* Data Protection checklist for Researchers - <http://www.intra.mdx.ac.uk/research-business/Research-ethics/index.aspx>

*This policy is due for review in November 2019*