

**Middlesex University Data Protection Policy**

|  |  |
| --- | --- |
| Policy owner | Legal Team |
| Author if different from above | N/A |
| Version | Version 2 |
| Last Review Date | 01/09/2022 |
| Next Review Due | March 2024, unless circumstances require an earlier review |

Approvals

|  |  |
| --- | --- |
| **Committee / Individual** | **Date** |
| Information Governance Group (IGG) | Approved by the Information Governance Group on 28 Nov 2022 |

**This data protection policy relates to obligations under the Data Protection Legislation, which includes the Data Protection Act 2018 (implemented by the General Data Protection Regulations [GDPR] )**

1. **Objectives and Scope 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 in relation to 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 and exercise any of the other individual rights are fully aware of how to do this and who to contact.
* Staff understand that subject access requests (and other relevant 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 using a Data Protection Impact Assessment to determine whether they will hold personal data, whether the system presents any privacy risks, damage or impact to individuals’ data and that it meets this policy’s requirements

This policy applies to all personal data and special categories of data (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. Further information on what is special category personal data can be found on the ICO website .

* This policy applies to all University employees, whether permanent, temporary, contractors, or consultants and students.
* 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 ICO registration reference is Z5439728**.**
* The following other companies will apply this policy as applicable: (i) MU Ventures Limited (ICO registration reference ZB192360) and (ii) MU Services Limited (ICO registration reference ZB192320).

1. **The data protection principles and individual rights**

The General Data Protection Regulation (GDPR) contains seven “Data Protection Principles” set out in Article 5. These specify that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary.
6. Processed in a manner that ensures adequate security of the personal data, using appropriate technical or organisational measures.
7. Take full accountability for what we do with personal data and how we demonstrate compliance.

Article 5(2) also sets out an overarching accountability principle ‘the controller shall be responsible for, and be able to demonstrate, compliance with the principles.’

**Individual rights** are set out in a separate part of the GDPR. In brief, the GDPR provides the following rights for individuals depending on the circumstances (and further detail on the individual rights listed below can be found in the ICO website):

:

* The right to be informed – Individuals have a right to be informed on how their data is being used, what the purpose is and the retention periods).
* The right of access – Also known as a Subject Access Request, individuals have a right to their own personal data.
* The right to rectification – Individuals have the right to have inaccurate information corrected.
* The right to erasure – Also known as the right to be forgotten, individuals have the right to have their data erased.
* The right to restrict processing – Individuals have the right to request their data be restricted.
* The right to data portability – Individuals have the right to their data being moved, copied and transferred to another IT system.
* The right to object – In certain circumstances individuals have the right to object to the processing of their data.
* Rights in relation to automated decision making and profiling. – Individuals have the right to know when automated decision making and profiling occurs, and have the ability to request for human intervention or challenge a decision.

1. **Policy Principles**

In order to meet the requirements of the data protection principles and individual rights set out in the GDPR, Middlesex University adheres to the following values when processing personal data:

**3.1 Fair Collection and Processing**

* The specific conditions contained in Article 6 and 9 of the GDPR 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 through relevant privacy notices;
* 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, where necessary;
* 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;
* It is important that we determine a lawful basis for processing any personal data. because the lawful basis for processing has an effect on individuals' rights;
* A ‘cease processing request’ (erasure 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 Data Protection Impact Assessment to be conducted, set out in the Data Protection Impact Assessment Policy. THE DPIA Policy can be found on the SLA intranet page.

**3.2 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. The Data Protection Officer will report any ‘serious’ breaches to the Information Commissioner’s Office as necessary, within 72 hours of the breach being reported internally;
* 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. It is mandatory for new staff to complete this training during induction. All staff have the opportunity to take the training as refresher training as regularly as they wish or as advised by the Data Protection Officer. The Data Protection Officer may also advise existing staff who have caused a data breach, or who have otherwise failed to comply with data protection law, or any aspects of the University’s data protection policies, to retake the data protection awareness training. The Data Protection Officer may advise staff on any training that may be useful to address any specific training needs of teams or of individual staff.

**3.3 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, where possible, 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 GDPR 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;
* As part of all relevant privacy notices 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 GDPR 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.

**3.4 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 and the final response and disclosure of information (subject to exemptions) will be given within the timescales required under the within 1 calendar month;
* 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. 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 GDPR, and is therefore exempt from disclosure under the Freedom of Information Act (Section 40).

**5. Data Protection responsibilities**

|  |  |
| --- | --- |
| **Who** | **What** |
| University as a corporate body | Data Controller |
| Board of Governors | Ultimately responsible for compliance with the GDPR. |
| Data Protection Officer | * 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. The University’s Senior Legal Advisor oversee data sharing agreements between the University and third parties. The University’s Senior Legal Advisor should approve data sharing agreements before they are entered into by the University; * Develop, administer, disseminate, review and support application of the policy. |
| Information Governance Group members | Support the Data Protection Policy and other related policies, procedures and guidance in terms of understanding and application within their respective Faculties/ Services. |
| Director of CCSS – on the specific responsibilities of the new Cyber Security Manager | Ensure adequate policies are in place for security of electronic information. |
| CDS | Nominated processor for all post sent to and within the University. |
| Line managers | Support and encourage staff to comply with the Policy.  Ensure that line reports process personal data in line with the requirements of the principles and individuals data protection rights. |
| 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 data protection principles and individuals data protection rights; * Bring queries and issues around data protection to the attention of the Data Protection Officer; * Do not attempt to gain access to information that is not necessary to hold, know or process; * Report subject access and other requests to Information Governance staff.   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 staff member as there is provision within the legislation to prosecute individuals for certain offences. |
| All students | Be familiar with the policy and comply with the policy where necessary.  Ensure that personal information provided is up-to-date and accurate.  Observe and comply with the data protection principles and individuals data protection rights.  Note that unauthorised disclosure of personal data will usually be a disciplinary matter. |