Produced by Information Governance Group
June 2018

General Policy Statement 4 (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 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

2. The data protection principles and individual rights

The General Data Protection Regulation (GDPR) contains six "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.

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:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

3. Scope of policy

- This policy has been written within relevant ICO guidelines.
- Definitions and terms used in relation to the GDPR can be found at https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- 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.
- 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 registration reference is Z5439728**.**

4. 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:

4.1 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 you determine a lawful basis for processing any personal data and document this. This becomes more of an issue under the GDPR because the lawful basis for processing has an effect on individuals' rights. 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 Data Protection Impact Assessment to be conducted. This is now a lawful requirement.

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. 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. Staff are strongly encouraged to complete this training during induction and subsequently on an annual basis.

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, 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.

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 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.

4.5 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 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 (John Gilchrist)	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.
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 – consultation 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. Compliance with data protection legislation and with the principles set

	out in this policy.
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 Information Governance 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 and the policy and comply 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.

6. Related policies and documents

All related internal Middlesex University documents can be found at the following link: https://www.intra.mdx.ac.uk/tools-policies/policies-and-guidance/information-governance/general-data-protection-regulation-gdpr

This policy will continue to be reviewed over the next 2 years as the new legislative framework for data protection in the UK matures.