MANCHESTER 1824
The University of Manchester

Data Protection Policy

If you are reading a printed version of this document, to ensure you have the most up to date version, you should check https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914.

1 Introduction

This Policy forms part of a suite of policies and procedures that support the Security and Privacy Framework.

The University needs to hold and to process large amounts of personal data about its students, employees, applicants, alumni, contractors and other individuals in order to carry out its business and organisational functions.

UK data protection law (UK GDPR plus the Data Protection Act 2018) defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This information is often referred to as person identifying information (PII) by the University and for the purposes of this Policy should be considered to have the same meaning as personal data as defined by the legislation.

2 Purpose

Compliance with legislation will be achieved through the implementation of controls and responsibilities including measures to ensure that:

2.1 personal data is processed lawfully, fairly and transparently. This includes the provision of appropriate information to individuals upon collection of their data by the University in the form of privacy or data collection notices. The University must also have a legal basis to process personal data and will record the policy and legal bases for processing;

2.2 personal data is processed only for the purposes for which it was collected. This will be achieved through Privacy Notices, Data Management Plans, Research Screening Assessments, Data Protection Impact Assessments and through Research Ethics Committees as well as assurance in relation to Data Protection clauses in contracts with suppliers;

2.3 personal data is adequate, relevant and not excessive for the purposes for which it was collected. This will be achieved through Privacy Notices, Data Management Plans, Research Screening Assessments, Data Protection Impact Assessments and through Research Ethics Committees as well as assurance in relation to Data Protection clauses in contracts with suppliers;

2.4 personal data is accurate and where necessary kept up to date. This will be achieved through Privacy Notices, Data Management Plans, Research Screening Assessments, Data Protection Impact Assessments and through Research Ethics Committees as well as assurance in relation to Data Protection clauses in contracts with suppliers;

MANCHESTER 1824
The University of Manchester

2.5 personal data is not kept for longer than necessary. This will be achieved through implementation of the University retention schedule in systems and in electronic and physical repositories where personal data is processed;

2.6 personal data is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that personal data, both manual and digital, are subject to an appropriate level of security when stored, used and communicated by the University, in order to protect against unlawful or malicious processing and accidental loss, destruction or damage. It also includes measures to ensure that personal data transferred to or otherwise shared with, or disclosed to third parties have appropriate contractual provisions and/or safeguards applied to maintain compliance with data protection law;

2.7 personal data is processed in accordance with the rights of individuals, where applicable. These rights are:

- the right to be informed;
- the right of access to the information held about them by the University (through a subject access request);
- the right to rectification;
- the right to erase;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights in relation to automated decision making and profiling;

2.8 The design and implementation of University systems and processes must make provision for the security and privacy of personal data, including a Data Protection Impact Assessment (DPIA) when the processing is likely to result in a high risk to the rights and freedoms of individuals. Processes and systems which use personal data will be screened to assess whether a DPIA is necessary;

2.9 Personal data will not be transferred outside of the UK without the appropriate safeguards in place;

2.10 Additional conditions and safeguards must be applied to ensure that more sensitive personal data (defined as Special Category data in the legislation), is handled appropriately by the University. Special category personal data is personal data relating to an individual's:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- health; or
- sex life or sexual orientation.

In addition, similar extra conditions and safeguards also apply to the processing of the personal data relating to criminal convictions and offences.

MANCHESTER 1824
The University of Manchester

3 Scope

This Policy applies to:

- all personal data held and processed by the University. This includes expressions of opinion about the individual and of the intentions of the University in respect of that individual. It includes data held in any system or format, whether electronic or manual;
- all personal data processed for University purposes in artificial intelligence software (including University supplied software such as CoPilot), in non-University owned SAAS applications (including free AI applications) and in social media applications
- all members of staff, as well as individuals conducting work at or for the University and/or its subsidiaries, who have access to University information (**"staff"**). This includes temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the University and suppliers (this list is not intended to be exhaustive); and
- all locations from which personal data is accessed including off-campus.

4 Responsibilities and compliance framework

All staff and other approved users of University systems must:

- complete data protection training every two years, and must seek advice and guidance from the Information Governance Office if clarification is required; and
- immediately report to the Information Governance Office any actual or suspected misuse, unauthorised disclosure or exposure of personal data, "near misses" or working practices which jeopardise the security of personal data held by the University.

Deans, Heads of School and Directors are responsible for ensuring that personal data within their areas is processed in line with this Policy and established procedures. To assist with this the University has identified Information Governance Guardians (IGGs) across all organisational units, areas and schools. Heads of School and Directors are also responsible for ensuring that there are an appropriate number of IGGs in their areas.

IGGs are responsible for overseeing data protection compliance in their areas, for providing a local point of contact for data protection issues, for identifying local training needs and arranging for them to be met and for disseminating advice and guidance from the Information Governance Office, including the Data Protection Officer. IGGs are also responsible for helping to identify circumstances where data sharing or transfer agreements are needed with third parties and ensuring that these are put in place.

The Information Governance Office is responsible for providing procedures, guidance and advice in support of this policy and for training staff and for conducting screening assessments, DPIAs, diligence in relation to data protection contract clauses and for managing data breaches and incidents which involve personal data. The IGO is also responsible for administering the servicing of data subject rights across the University

The Data Protection Officer is responsible for overseeing the University's compliance with the data protection legislation.

Staff must note that any breach of this Policy may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action or sanctions. Serious

breaches of this Policy may constitute gross misconduct and lead to summary dismissal or terminal of contract.

5 Monitoring compliance

This Policy and its implementation are subject to internal monitoring and auditing throughout the University, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. The University will also undertake appropriate benchmarking and may be audited by external bodies.

Reports on matters related to this Policy will be provided to the Information Governance Committee.

6 Review of Policy

This Policy will be reviewed at least annually or when significant changes are required.

MANCHESTER 1824
The University of Manchester

Version amendment history

Version	Date	Reason for change
1.0	October 2012	Creation and approval by the Board of Governors
1.1	Nov 2014	Links updated
1.2	June 2017	Data Protection Guardians changed to Information Governance Guardians; Records Management Office changed to Information Governance Office
1.3	December 2017	Amendments related to change in legislation; consistency with other policies
1.4	January 2018	Inclusion of: 2year DP training requirement for all staff per PRC; sanctions per REMG – approved by IGC 23 January 2018
1.5	24 Jan 2018	Changed Special Category data list to be consistent with GDPR list as requested by HOIG; minor amendments from OGC – sent to PRC for endorsement on 6 Feb 2018
1.6	6 Feb 2018	Amendment to IGG role requested at IG Sub-committee
1.7	8 June 2018	Minor amendment to 2.8 to explicitly reference DPIA
1.8	12 Dec 2018	Links updated
1.9	22 March 2021	Minor amendments to 1 and 2.9 to reflect UK law post exit from the EU and 2.6 to clarify disclosure requirements
2.0	29 April 2025	Amendments approved by IGC: Inclusion of AI (including CoPilot) SAAS and Social Media, explanation of methods used to ensure compliance, explication of responsibilities of IGO, reference the UoM AI Guidelines.

Document control box	
Policy title:	Data Protection Policy
Date approved:	23 Jan 2018
Approving body:	Information Governance Committee
Version:	2.0
Supersedes:	1.9
Previous review dates:	June 2022
Next review date:	April 2026
Related Statutes, Ordinances, General Regulations:	Ordinance 14 Intellectual Property Rights, Data Protection and the Use of Information Systems; University General Regulation XV Use of Information Systems; Statute XIII Part III disciplinary procedures for staff
Equality relevance outcome:	Medium
Related policies:	Information Security Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525 Records Management Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14916 Freedom of Information Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14915 Acceptable Use Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16277

Related procedures:	Information Security Classification, Ownership and Secure Information Handling SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 Records Retention Schedule: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514 Other related policies and procedures: http://www.staffnet.manchester.ac.uk/igo/policy-procedures/
Related guidance and/or codes of practice:	Information Governance guidance: https://www.staffnet.manchester.ac.uk/igo/ IT Security guidance: http://www.itservices.manchester.ac.uk/secure-it/ AI (Artificial Intelligence) Guidelines: https://www.staffnet.manchester.ac.uk/dcmsr/communications/ai-guidelines/
Policy owner:	Executive Director of Compliance and Risk
Lead contact:	Director of Information Governance