

INFORMATION MANAGEMENT POLICY



This document sets out the policy governing the publication, retention and disposal of the University's records.

Version	1.2
Executive Sponsor	Chief Operating Officer
Officer Responsible for Policy/ Procedures	General Counsel
Consultation Process	Information Security and Compliance Group
Date of Approval and Committee and/or Executive Officer	Executive Operations Group Executive
Effective Date	1 February 2021

INTRODUCTION AND CONTEXT

The University's information needs to be effectively managed in order to support the delivery and management of its core function, and to comply with its legal and regulatory obligations, including its transparency obligations under the Freedom of Information Act 2000.

This document sets out the policy governing the publication, retention and disposal of the University's records and specifically in relation to those records including personal data and records required for the purposes of legal risk management.

Records may be retained for business needs only to the extent permitted by this Policy. Certain agreed policies and datasets will be published on the University's website under the Publication Scheme.

This Policy applies in the context of the Privacy Policy and more particularly the University's strategic objectives to minimise its use of personal data, delete personal data without delay when it is inaccurate and keep personal data in an identifiable form only for as long as necessary to fulfil the purposes for which the University collected it.

1. SCOPE OF THE POLICY

1.1 Purpose of the Policy

The purpose of this Policy is to establish consistent and robust controls and accountability for:

- the retention and disposal of the University's electronic and paper-based records which are in accordance with relevant legislation and the Privacy Policy; and
- the publication of certain of the University's records in compliance with its transparency obligations under the Freedom of Information Act 2000 and the Information Commissioner's Office guidance through the Publication Scheme.

1.2 What is covered by the Policy

This Policy applies to all University records; that is records created, received or maintained by the University in the course of carrying out its business, including the carrying out of research and the fulfilment of compliance with any regulatory requirements.

The records may be in any format or medium, including electronic documents, emails, text and social media channels. They may also be stored, managed or hosted elsewhere so agreements of this nature should ensure such arrangements comply with this Policy.

A small proportion of the University's records may be selected for permanent preservation to give a lasting record of the University's business. Any such retention will be subject to the Privacy Policy, this Policy and will be agreed in consultation with the General Counsel.

Certain records will be published in accordance with the Publication Scheme.

1.3 Who is covered by the Policy

All those who access personal data held by the University including staff must be aware of and comply with the Policy. This Policy does not form part of any contract of employment and may be amended at any time.

1.4 Breach of this Policy

Any breach of this Policy and its associated procedures by staff will be investigated in accordance with the University's disciplinary procedure. A serious breach may amount to gross misconduct, and could therefore result in summary dismissal.

Any breach of this Policy and its associated procedures by non-staff will be investigated and steps taken in accordance with the law and any relevant contract.

1.5 Policy Ownership

The Executive has approved this Policy, the Chief Operating Officer is the Executive sponsor and the General Counsel is the officer responsible for the Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the General Counsel. The General Counsel is the University's designated statutory Data Protection Officer in accordance with the requirements of the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

2. THE POLICY STATEMENT

The guiding principles of this Policy are to ensure that the University maintains, publishes and destroys its records in a manner that allows it to meet its business needs, manage its legal risks and comply with the law, particularly in relation to transparency and data protection.

Those who access records held by the University, including staff, are required to complete the training required under the Privacy Policy, or substantially similar training, to inform them about personal data law so they will have an appreciation of the importance of compliance with this Policy. The Records Management Procedures and the Publication Scheme implement this Policy.

Compliance with this Policy will result in:

- records that give accurate and relevant information on the University's transactions;
- records that are authentic and reliable;
- records that are stored within suitable filing systems, enabling easy retrieval and avoiding unnecessary duplication;
- access to records that are balanced with security appropriate to their level of confidentiality and importance;
- records being retained for the correct length of time, and disposed of appropriately in line with the Records Management Procedures; and
- transparency in relation to the five areas covered by the Publication Scheme (governance and compliance, policies and regulations, student data, staff data and procurement and suppliers).

3. RELATIONSHIP TO EXISTING POLICIES

This Policy should be used in conjunction with other relevant University policies and documents including:

- Privacy Policy and its associated procedures;
- Records Management Procedures;
- The Publication Scheme;
- IT Security Policy; and
- Research Data Management Policy.

Records should also comply with any external guidelines, policies or legislation, including the requirements of the Information Commissioner's Office, the Office for Students, the research councils, ERDF, other funders of research and any audits.

Please contact the Office of the General Counsel if any conflict is identified between the University's policies and procedures and any external guidance.

4. IMPLEMENTATION AND RESOURCES

It is expected that Colleges and Departments will implement practices to ensure compliance with this Policy, and review them regularly. It is the responsibility of the record owner to ensure that good housekeeping practices are undertaken to ensure the accuracy and relevance of information assets that reside on the University servers. It is strongly advised that any personal or residual information or personal data that has no value or is no longer required for University purposes should be removed from the relevant drives and servers on a regular basis and in accordance with the IT Security Policy.

The Records Management Procedures provide a list of the records produced by the University, and details of the length of time that they should be retained to meet operational and regulatory requirements. It assigns staff responsibilities for the management of records, and provides the rationale for the recommended time periods, with details of any legislative or archival value considerations.

Colleges and Departments are required to review records at the appropriate time and, once records are approved for disposal, destroy these records. Paper records if confidential, and/or include any personal data, must be disposed of using the confidential waste disposal service. Where records are not confidential and/or do not contain personal data, they can be destroyed in the "non-confidential" paper bins. Electronic records should be deleted, ensuring that all versions and copies are destroyed.



Aston University
Birmingham
B4 7ET, UK

+44 (0)121 204 3000
aston.ac.uk

