UNIVERSITY OF ABERDEEN

RECORDS MANAGEMENT POLICY

1. Purpose

This policy sets out the guiding principles and responsibilities for managing the University's records of its activities. The policy is designed to ensure records are managed efficiently and effectively to support University functions, to comply with legal and accountability requirements, and to preserve an enduring record of significant University activities.

2. Scope

This policy and its supporting guidance apply to all University records. Records are defined as recorded information that is created, received or maintained by the University, or on behalf of the University, as evidence of its actions, decisions and transactions in the conduct of its business activities.

The policy applies to records in any format (paper and digital), media type or location, and to all activities resulting in the creation, receipt, use, distribution, maintenance or disposal of those records. This includes but is not limited to:

- emails that record the University's business actions and decisions;
- research records created by staff in the course of their research, whether internally or externally funded;
- information in all systems in which University records are created, received, processed and stored, including mobile devices; and
- records created by University staff operating in University overseas campuses, with due regard for non-UK legislation that may be applicable.

The policy applies to the management of University records throughout their lifecycle stages; from creation or capture, through active use, to final disposal, whether the record is destroyed or selected for permanent retention.

This policy applies to all staff employed by the University and to third party partners and suppliers who share, manage and process information on behalf of the University.

3. Roles and responsibilities

The roles that carry responsibilities under this policy are as follows:

- Heads of Schools and Directors of Professional Services are responsible for the management of all records generated, processed and held within their school or service, for promoting good practice in records management, for the transfer of records of historical value to the University archive and for effective implementation of this policy within their areas of responsibility. Heads of School and Directors are supported in their schools / directorates by nominated information champions.

- Staff are responsible for ensuring the accuracy, integrity and reliability of records they create, receive, process or share on behalf of the University; and for the disposal of records in accordance with the University retention schedules.
- The Information Governance team are responsible for developing records management policy, procedures and retention schedules, providing training and guidance to staff and supporting compliance with this policy and its supporting policies, procedures and guidance.
- The Data Protection Officer has statutory remit to monitor the University's compliance with the UK General Data Protection Regulation and the Data Protection Act 2018, including the requirement that personal data is not kept for longer than necessary.
- Special Collections are responsible for maintaining the University archive.
- The Information Governance Committee has executive responsibility for records management compliance within the University of Aberdeen, and for taking steps to address risks and issues of concern. The Committee has authority to approve updates to the retention schedules for University records to reflect business, legislative or regulatory requirements.
- The Information Risk Working Group is responsible for reviewing information governance and security risk and advising on risk treatment efforts and consistent implementation of this policy.

4. Principles

4.1 The University shall create, receive, and maintain information assets that:

(1) are **Authentic**; **Reliable** and have **Integrity**. Information assets are reliable, authentic, accurate, complete, and protected from unauthorised amendment or deletion, so that they can be trusted. They can be proven to have been created or sent by those who have purported to have created or sent them and at the time purported and processes are in place for the secure disposal of information assets. For example, adequate audit trail and version history metadata is created and maintained, and evidential weight is maximised, so the University meets its audit and regulatory obligations. It is clear where the Single Point of Truth is held, who is responsible for its maintenance, and any copies are clearly identified as such. Where appropriate, information quality standards are defined and monitored so that it can be relied on for evidence-based decision-making.

(2) are **Useable**. Information assets are consistent, fit-for-purpose and support the achievement of the University's 2040 Strategy. For example, the University shall avoid creating or collecting unnecessary information; avoid unnecessary duplication; and seek to avoid any information gaps that hinder the ability of the University to achieve the University's objectives and meet legal requirements. Where appropriate and lawful, information is standardised, comparable and linkable to allow it to be reused so that the University can maximise its value.

(3) have **Confidentiality**. Information assets are protected from unauthorised access, disclosure, alteration, and destruction. They are as closed as necessary and as open as possible. For example, by applying role-based access permissions that are assigned and rescinded promptly in accordance with business need. The University will ensure that records are protected in the way that they are accessed, stored and shared, regardless of format, system or location.

(4) have a defined **Lifecycle**. Information assets have a defined lifecycle that allows the University to retain them as long as required – but no longer – and to explain why and how long we retain specific information assets. This includes identifying information assets with archival value as early as possible so that they can be preserved permanently. Information lifecycles are defined in the University's Retention Schedules, which support this Policy. The University will retain permanently an archive of records of enduring legal, administrative, education, research or other historical value.

(5) are **Available**. Authorised individuals know what information assets exist and can locate and retrieve them timeously throughout their lifecycle and thereafter they can be presented and interpreted. For example, it is possible to identify and retrieve all the information about a specific individual to facilitate their data subject rights. The information assets are clear, concise, intelligible, and legible. They are usable by any University personnel authorised to do so, taking into account accessibility requirements.

(6) are **Resilient**. Information assets are resistant to the impact of incidents that would otherwise have a serious adverse impact on their confidentiality, integrity or availability, and support business continuity. The University will identify critical business records, vital for business continuity, and maintain appropriate backup and disaster recovery procedures to minimise the negative impact to the University and individuals in the event of loss or destruction.

4.2 In order to comply with the Principles, the University use and management of the information assets is:

- **Proportionate** The University's use and management of information is proportionate to the purpose, benefits, and costs, and takes account of the University's risk appetite.
- **Risk Assessed** The University is aware of the risks that would be entailed by failure to have authoritative records of activity and documents the risks if the information asset is lost or compromised.
- **Legal and Compliance** The University's use of information complies with the privacy laws in all the jurisdictions in which it operates including UK privacy laws.
- **Accountable** The University creates, keeps, and manages information to support its business activities and to be accountable for its actions and decisions, including compliance with legal obligations, regulatory requirements and community expectations. Information Asset Owners are accountable for the governance and management of

information assets produced and maintained by the functions and activities for which they are accountable.

• **Cost-effective** The University's use of information, and its information systems balance economy, efficiency, and effectiveness to achieve the University's 2040 Strategy with the optimal use of resources and are value for money over the long-term. For example, information assets are held in the medium most appropriate for the task they perform, in the most cost-effective location, and wherever possible and practicable routine information management activities are automated to support staff and make processes more effective and efficient. Information sources are integrated rationally so manual keying between systems is minimised.

• **Sustainable** The University's use of information is socially responsible and reflects the University's ethos, values, and heritage. For example, the use of information supports the University's Sustainability Commitments with a particular focus on retaining paper and electronic information assets only for as long as required and disposing of these timeously and appropriately.

• **Transparent** The University is transparent about its activities, the purposes for which it holds information and how that information is managed. University information is discoverable where lawful to do so and potentially disclosable, for example in response to freedom of information requests and data subject rights requests.

• **Reviewed** The University identifies and evaluates opportunities for improving the effectiveness, efficiency or quality of its processes, decisions and actions that could result from better records creation or management.

4.3 Information and Records Management Plan

The University is undertaking an Information and Records Management Plan (IRMP) to enable the application of the data handling principles and ensure the management of our information assets. The plan will deliver effective and efficient management of information by ensuring that all relevant information and processes are recorded and kept up-to-date including the Information Asset Register and Record of Processing Activities. This will highlight areas of risk involving data management, identify core business assets across the University and ensure compliance with data protection legislation. The IRMP will be a collaborative process with all roles, as outlined in section 3, playing a part in the process.

5. Related policies

The Data Protection policy sets out the guiding principles and responsibilities for managing personal data in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018.

The Information Security policy and procedures set out the means by which information shall be secured to protect it against the consequences of breaches of confidentiality, failures of integrity, or interruptions to its availability.

6. Review and Development

This policy shall be reviewed on an annual basis by the Information Governance team and, if required, recommendations for amendment made to the Information Governance Committee.

Approval/Review History

Version	Date	Action
1.0	University Court, 29 June 2004	Approved
2.0	University Court, 22 May 2007	Approved
2.0	Information Security Committee, May 2009	Reviewed
2.1	University Records Manager, 1 June 2015	Minor updates
2.2	University Records Manager, 1 June 2016	Minor updates
3.0	Operating Board, 6 March 2019	Approved
3.0	University Data Protection Officer, February 2020	Reviewed
4.0	Information Governance Committee, 2 March 2021	Approved
5.0	Information Governance Committee, 6 April 2022	Approved
5.1	Information Governance Committee, 23 March 2023	Approved
6.0	Information Governance Committee, 4 March 2024	Approved

Policy Metadata

Metadata element	Metadata
Title	Records Management Policy
Author / Creator	Data Protection Officer
Owner	Director of Digital and Information Services
Date approved	4 March 2024
Version	6.0
Reviewed	February 2024
Date of next review	March 2025
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University
Related documents	Data Protection Policy Information Security Policy Research Governance Handbook
Subject / Description	The principles and responsibilities for managing records and handling information effectively.
Document status	Policy
Equality Impact Assessment	N/A
Theme	Information Management

Metadata element	Metadata
Keywords	Records, governance, information, retention, corporate, accountability, compliance, risk, security, privacy, data