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 applies 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:

- 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.

- 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.

4. Principles

(1) The University will facilitate easy, fast and secure access to reliable information to save staff time and effort.

(2) The University will maintain the integrity, authenticity, reliability and usability of University records over time.

(3) 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) The University will ensure that records are protected in the way that they are accessed, stored and shared, regardless of format, system or location.

(5) The University will keep records only for as long as required and then authoritatively dispose of them when they cease to be of business or compliance value.

(6) The University will retain permanently an archive of records of enduring legal, administrative, education, research or other historical value.

5. Related policies

The Data Protection policy sets out the guiding principles and responsibilities for managing personal data in accordance with the 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
V1.0	University Court 29 June 2004	Approved
V2.0	University Court 22 May 2007	Approved
V2.0	Information Security Committee May 2009	Reviewed
V2.1	University Records Manager 1 June 2015	Reviewed/minor updates
V2.2	University Records Manager 1 June 2016	Reviewed/minor updates
V3.0	Operating Board 6 March 2019	Approved

Policy Metadata

Title	Records Management Policy
Author / Creator	Iain Gray, Data Protection Officer
Owner	Director of Digital and Information Services
Date published / approved	
Version	V 3.0
Reviewed	January 2019
Date of next review	January 2020
Audience	All staff, partners, suppliers and contractors who work for or on behalf of the University
Related documents	Data Protection Policy Information Security Policy Business Continuity 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
Keywords	Records, governance, information, retention, corporate, accountability, compliance, risk, security, privacy, data