



## RECORDS MANAGEMENT POLICY

### 1. Introduction

1.1 The University is subject to numerous pieces of legislation and regulation which govern the management and retention of records, and is also obliged to conform with the “Scottish Ministers’ Code of Practice on Records Management by Scottish Public Authorities under section 61 of the Freedom of Information (Scotland) Act 2002” (“FOISA s.61 Code of Practice”).

1.2 Records are created, received and used by University employees, associates and agents in the process of undertaking University business functions and activities, and are important sources of administrative, financial, legal and historical information. They are essential to the functioning of the institution in its current and future operations and should, therefore, be considered to be corporate assets and managed appropriately throughout their lifecycle for the purposes of accountability and evidence of decisions and transactions.

1.3 Good records management benefits the University by supporting legal and regulatory compliance, reducing risk and enabling the efficient and effective conduct of business.

### 2. Definitions

2.1 Records are: “any recorded information, irrespective of format, created or received, and maintained by an organisation or person in the transaction of business or conduct of business affairs and kept as evidence of such activity” (ISO 15489:1:2001)

### 3. Purpose

3.1 The purpose of this policy statement is to provide a framework for the creation, management and disposal of records within Edinburgh Napier University.

3.2 Ensuring good records management practices are embedded across the University mitigates the associated risks, as detailed in the FOISA s.61 Code of Practice, including:

- Financial or reputational loss if recorded evidence is not available or reliable,
- Poor decisions based on inaccurate or incomplete information
- Inconsistent or poor levels of service
- Non-compliance with statutory, regulatory or sector requirements,
- Failure to protect vital information leading to inadequate business continuity planning,
- Failure to protect the rights of stakeholders

3.3 To ensure that records management practices align to Strategy 2020 and the University's Values, specifically:

- **Build Innovation, Enterprise and Citizenship**
  - Adopt a continuous improvement/enhancement approach in all that we do
  - Maximise the value of our [information] assets

#### 4. Scope

4.1 This Policy Statement applies to all employees (including short-term or casual and student employees), associates and contractors employed by the University who process (create, receive, use, retain/maintain and dispose of) University records ("employees").

4.2 This Policy Statement covers all University records processed in the course of employment with the University, in any location e.g. on or off University premises, and in any format, e.g. physical and electronic, including those in information systems such as database applications and email.

#### 5. Policy Statement

5.1 The University is committed to:

- Compliance with the legislation and maintaining a framework of policies and procedures to support both legislative compliance and good records management practices and procedures,
- Ensuring all employees are aware of their responsibilities with regard to the management of University records,
- Establishing and maintaining record-keeping practices that meet its operational needs, accountability requirements and stakeholders' expectations,
- Providing training and guidance resources to promote compliance and good records management practices.

5.2 The University requires all employees to:

- Comply with the legislation, policy and best practice recommendations,
- Create records which are high quality, accurate, reliable and useable,
- Maintain University records in storage which has appropriate security controls and is accessible to authorised colleagues – for electronic records this is a shared network area with appropriate permissions, the same principals apply for physical records. Records should not be stored in personal areas which appropriate colleagues cannot access e.g. H:Drive, C:Drive (desktop), Sharepoint personal sites, Outlook (or other email), personal mobile device/PC, at home, etc. Records must be maintained in such a way that they can be easily found and retrieved when required e.g. filed/classified according to the activity to which they relate with appropriate naming conventions.
- Ensure records are disposed of in accordance with approved University Records Retention Schedules.

## **6. Responsibilities**

6.1 All employees and agents acting for and on behalf of the University are responsible for managing any records they create, receive and subsequently use in the course of their employment in accordance with legislation, regulation and best practice recommendations as set out in this policy.

6.2 All line managers are responsible for ensuring that records created, received or used in the course of the University's business in their area of responsibility conform to the requirements of this policy and all allied legislation, regulation, policy and procedures. Managers must ensure that all employees reporting to them are aware of this policy and their individual responsibilities in managing the University's records. Managers must ensure that sufficient records management procedures are in place for their area of responsibility. Training needs must be identified and arranged as necessary e.g. as part of the My Contribution process. Managers must ensure that the vital records for which they are responsible are identified, adequately protected and included in the appropriate Business Continuity Plans and Business Impact Analyses.

6.3 Governance Services are responsible for the provision of records management guidance and training.

6.4 Deans of Schools and Directors of Service Areas are responsible for ensuring that adequate resources and support mechanisms are available to enable employees to comply with the requirements of this policy.

6.5 The University Secretary has overall responsibility for ensuring the University complies with information legislation.

## **7. Sanctions for Non-Compliance**

7.1 Failure to comply with this policy may lead to the relevant disciplinary procedures being invoked.

## **8. Legislation and Associated Policies**

8.1 [Data Protection Policy Statement and Code of Practice](#)  
[Information Security Policies](#)

8.2 The main pieces of legislation governing records management are:  
Civil Evidence (Scotland) Act 1988  
Consumer Protection Act 1987  
Copyright, Designs and Patents Act 1988  
General Data Protection Regulation and Data Protection Act 2018  
Equality Act 2010  
Financial Service Act 1986

Freedom of Information Act (Scotland) 2002  
Prescription and Limitation (Scotland) Act 1973 and 1984  
Value Added Tax Act 1994 (HMRC 700/21: keeping VAT records)

- 8.3 Further detail about applicable legislation is available online at:  
<https://staff.napier.ac.uk/services/governance-compliance/governance/records/Pages/RecordsManagementLegislationandStandards.aspx>

## 9. Contact

- 9.1 Queries about this Policy can be directed to:  
Governance Services - <https://staff.napier.ac.uk/services/governance-compliance/Pages/who.aspx>

<b>Document Control Information</b>	
Title	Records Management Policy
Version	V2.3
Author	Governance Services
Date Approved	First approved (V1.0): 2010 by CMT Second review and approval: 13 October 2015 by UIGG (major update) Second review: 21 February 2017 by UIGG Third review: 29 October 2019 by UIGG
Review Date	Biennially
Scope	All University employees