



**University College Cork**  
**– National University of Ireland, Cork**

**Records Management Policy**  
**Version 1.0**

## Table of Contents

<b>1</b>	<b>Purpose</b> .....	<b>3</b>
<b>2</b>	<b>Scope</b> .....	<b>3</b>
<b>3</b>	<b>Policy Requirements</b> .....	<b>4</b>
<b>3.1</b>	<b>All Processing Activities</b> .....	<b>4</b>
<b>3.2</b>	<b>Records Retention Schedules</b> .....	<b>4</b>
<b>3.3</b>	<b>Day-to-Day Recordkeeping Processes</b> .....	<b>4</b>
<b>3.4</b>	<b>Digital Records Systems: Archival Preservation, Records Management, and Data Transfers</b> .....	<b>5</b>
<b>3.5</b>	<b>Version Control and Minimisation of Duplication</b> .....	<b>5</b>
<b>3.6</b>	<b>Staff Leaving the University</b> .....	<b>5</b>
<b>4</b>	<b>Roles and Responsibilities</b> .....	<b>5</b>
<b>5</b>	<b>Non-compliance with Policy</b> .....	<b>7</b>
<b>6</b>	<b>Supporting Documentation</b> .....	<b>7</b>
<b>7</b>	<b>Further Information</b> .....	<b>7</b>
<b>8</b>	<b>Disclaimer</b> .....	<b>7</b>
<b>9</b>	<b>Definitions</b> .....	<b>8</b>
<b>10</b>	<b>Appendix: Data Owners Table</b> .....	<b>9</b>
<b>11</b>	<b>History and Approval</b> .....	<b>10</b>

## 1 Purpose

University College Cork ('the University') is committed to the proper and effective management of the records and data it creates, receives, captures, maintains, or otherwise processes, in all formats, in the course of its operations, academic and administrative, in a manner which:

- is transparent, consistent, and accountable;
- meets legal, regulatory, and audit requirements;
- supports the efficient conduct of its business;
- protects the security and integrity of Records and Data, including Personal Data;
- ensures the preservation of Archives documenting its history and development.

The University recognises that records management is a collaborative process, which calls for the support and active participation of management and staff at all stages, including design, implementation, compliance, and review. Engagement is essential to achieving the purposes of this Policy.

It is acknowledged that the greater part of the University's records is now held in digital formats, including records comprised of data within digital systems. The University commits itself to ensuring its record systems, for both digital and hard copy records, support records management processes and the purposes of this Policy.

Particular recognition is given to the University's obligations as a data controller and processor towards data subjects under the University's [Data Protection Policy](#) and Data Protection legislation, and to the special and limited derogations given under that legislation for processing data for research and statistical purposes, and for archival purposes in the public interest.

Records management processes will respect the University's principles of [academic freedom](#).

In seeking to manage its records and to preserve its digital archives and associated metadata appropriately, the University will have regard to ISO 15489, the International Standard for Records Management, and to the principles of ISO 14721, the reference model for an Open Archival Information System (OAIS).

## 2 Scope

This Policy applies to all records, in all formats, created, received, maintained or otherwise processed in the course of the activities of the University including, without limitation, hard copy and digital records.

Personal records unrelated to University activities are not within the scope of this policy. Staff are advised to avoid maintaining such records within University systems (eg, email servers, network folders), as doing so may place them within the scope of legislation such as Freedom of Information.

Research Data is subject to the University's [Research Data Management Policy](#).

## 3 Policy Requirements

### 3.1 All Processing Activities

All Users processing records or data created in the course of the University's activities must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times. They must comply with the relevant policies of the University (as may be amended from time to time) and with all applicable legal requirements, particularly in relation to data protection and copyright.

### 3.2 Records Retention Schedules

Records Retention Schedules (RRS) have been developed through collaboration with Staff in each Functional Area, have been agreed with management, have been approved by Data Owners, and must be applied to the management of records in each area.

#### **Changes to RRS**

Changes to RRS, including for example the addition of new records series, changes to disposal periods or actions, may only be made by the University Archivist, who is responsible for maintaining the master set of RRS.

Staff, Students, and Other Users should bring questions and information about potential or required changes to RRS to the University Archivist's attention. Changes made must be approved by the relevant Data Owner. These processes are subject to a change control procedure.

#### **Exceptions to disposal actions in RRS**

Where records liable for destruction or deletion are relevant to an ongoing or pending formal process, such as an appeal, an audit, an investigation, a formal information request, or legal proceedings, disposal action must be suspended until that formal process has terminated.

Intentionally destroying or altering a record relevant to such a process may be an offense in law.

Staff should notify their Head of Functional Area in writing of the suspension of disposal action, the reason for it, and, subsequently, its termination, in line with an exceptions procedure.

### 3.3 Day-to-Day Recordkeeping Processes

Records and data are to be named, saved, and stored in a manner consistent with the records series<sup>1</sup> set out in the RRS applicable in one's area, so that it may be clear to which series a record belongs. For example, the filing tree structure on an area's main network drive may mirror the records series set out in the retention schedule.

Staff must follow all University Records Management procedures and be aware of related guidelines, and should, where relevant, inform Students and Other Users of their responsibilities under this Policy.

Functional Areas must also have in place local procedures and standard operating procedures, for systems and practices specific to their area. They must ensure that local procedures are consistent with this Policy and its underlying procedures, and with related University policies and procedures.

---

<sup>1</sup> A records series is a defined grouping of related records subject to the same retention/disposal actions, as set out in a records retention schedule

### 3.4 Digital Records Systems: Archival Preservation, Records Management, and Data Transfers

The ongoing preservation requirements of records identified as being of archival or permanent value must be addressed at all stages of the records' life-cycle. Regular back-ups, system audits, and controlled migration and conversion of data and supporting metadata during upgrades and systems changes, are all essential steps.

Staff involved in the procurement, development, upgrading, or termination of enterprise and other systems used for digital records must consider the records management implications of these processes, and must ensure that the purposes of this Policy are met. It is recommended that IT Services be consulted at the planning stage. Other offices including the Procurement Office, the University Archives, and the Information Compliance Office may also be consulted where relevant.

Processes involving the transfer of personal and commercially sensitive data across networks and copying to other media must safeguard their confidentiality and integrity, eg, through encryption.

The removal off-site of personal or commercially sensitive data, or records containing such data, must be authorised by the Data Owner, and must similarly be carried out in a manner which safeguards against the risk of theft, loss, or data breach.

The Data Custodian (eg IT Services) can advise on [data security](#) and [safeguarding measures](#).

### 3.5 Version Control and Minimisation of Duplication

Effective version control has been identified by the University as best practice, supporting data quality, reducing uncontrolled distribution, and allowing for deletion of earlier versions once superseded where permissible under the RRS (see [Guideline on version control](#))

Minimisation of duplication is a key component of the University's records management processes. Master records and data sets are to be held by relevant areas as identified in the RRS. Other areas should not generally hold copies of such records and data. Where they need to do so, the records and data concerned should be held for a limited time and stated purpose, consistent with [procedure](#) and the relevant RRS.

### 3.6 Staff Leaving the University

Staff leaving the University, or changing positions within it, must leave all University records for the use of staff and successors within the relevant area.

## 4 Roles and Responsibilities

**University Management Team (UMT)** endorse this Policy and take institutional responsibility for ensuring implementation and compliance.

**All staff** are responsible and accountable for creating and keeping accurate and complete records of their business activities. This includes records and data created in the course of carrying out or contributing to research (see [Research Records Management procedure](#)).

Staff must ensure that the records and data for which they are responsible are securely managed in a manner which is compliant with this Policy, related [University policies](#), and [relevant procedures](#), including the [Data Protection Policy](#), [IT Security Policy](#), [Data Classification Procedures](#), and [External Hosting Policy](#).

The processing of personal data is subject to data protection legislation. The obligations of those processing such data in the course of University business are set out in the University's Data Protection Policy.

**Designated staff members** may be appointed by Data Owners to take day-to-day responsibility for records management processes (eg, security, transfer, disposal), to support other staff in performing such processes, to report to management, and to liaise with the University Archivist.

The identity of designated records management staff members should be recorded and known to all staff in the relevant unit. The general functions of designated records management staff are set out in a guideline.

**Data Owners** are generally the most senior person in a functional area, and are responsible for the records and data processed in or on behalf of their area. Examples of Data Owners include the Registrar (student records), the Bursar (financial records), and Director of HR (human resources records). The Data Owners for each records series are set out in Records Retention Schedules (RRS) (see also appendix below).

Data Owners have overall and operational responsibility for records management implementation and compliance within their functional area or area of work. This includes the following:

- authorising access to and processing of records and data and assigning responsibilities;
- ensuring adequate training and guidance is given and facilitated;
- managing risk and ensuring appropriate security and recovery arrangements are in place;
- approving actions as required under records management procedures and RRS;
- ensuring standard and local procedures, eg, for digital systems used in their area, are applied, and developed where necessary;
- ensuring processing activities carried out on their behalf (see below) comply with this Policy and other relevant University policies, all applicable legal requirements, and any applicable contract or agreement.

Where processing activities are carried out on behalf of the Data Owner by Data Custodians or Data Processors<sup>2</sup>, all parties must provide each other with any information necessary to fulfilling their responsibilities. The Data Owner retains overall responsibility for the records or data concerned.

Where a Data Controller engages a Data Processor to carry out processing on its behalf, there is a statutory requirement that a contract in writing between the parties be entered into, governing those processing activities.

**Data Custodians and Data Processors** who process records or data on behalf of a Data Owner have certain responsibilities, including the following:

- ensuring that they protect the integrity, confidentiality, and security of records and data entrusted to them;
- ensuring that access and processing is restricted to what is authorised by the Data Owner

Where **Students and Other Users** process and/or gain access to records and data created in the course of University activities, they are subject to the requirements of this Policy relating to All Processing Activities (above). Attention is directed to relevant guidelines.

---

<sup>2</sup> See 'Definitions' (below)

**The University Archivist** is responsible for maintaining and reviewing this Policy and records retention schedules, and for promoting a culture of good records management practice.

## 5 Non-compliance with Policy

Failure to comply with this policy is a breach of University regulations and may be the subject of disciplinary action in accordance with the University's disciplinary procedures.

## 6 Supporting Documentation

The Policy should be read in conjunction with the following University policies, procedures and guidelines. Staff must ensure their compliance with these policies and procedures in addition to this policy.

[Data Protection Policy](#)

[Data Classification Procedure](#)

[IT Security Policy](#)

[Acceptable Usage Policy](#)

[Externally Hosted Personal Data Policy](#)

[Records Management Procedures](#)

[Records Management Guidelines](#)

[Data Protection Procedures and Guidelines](#)

This Policy is subject to the University's [Principal Statute](#) and to the University's [Policy Framework](#).

[Records management procedures and guidelines are presently being updated. Hyperlinks to these and other supporting documentation will be added in due course.]

## 7 Further Information

Queries regarding this Policy or Records Management at the University should be directed to the University Archivist: [archives@ucc.ie](mailto:archives@ucc.ie); Tel. +353 (0)21 4902753; University Archivist, UCC, 6 Elderwood, College Road, Cork, T12 VH39.

## 8 Disclaimer

The University reserves the right to amend or revoke this policy at any time without notice and in any manner in which the University sees fit at the absolute discretion of the University or the President of the University.

## 9 Definitions

In the context of this Policy, capitalised terms used throughout shall have the following meanings:

### **University:**

“The University” means University College Cork – National University of Ireland, Cork

### **Policy**

“Policy” means this Records Management Policy

### **Functional Area**

“Functional Area” means area of University operations ordinarily headed by a member of the University Management Team, specifically the Vice-Presidents, Heads of Colleges, the Bursar, the Corporate Secretary, and senior Directors, as set out in the University’s organisational structure.

### **Heads of Functional Areas**

“Heads of Functional Areas” are ordinarily members of the University Management Team (UMT) and are the most senior person in their functional areas, as set out in the University’s organisational structure.

### **Data Owner**

“Data Owner” ordinarily means the most senior person in the functional area within which the data is created or stored unless this role has been explicitly and formally delegated to someone else by the most senior person in the aforementioned areas. The Data Owner for each records series is set out in records retention schedules.

### **Data Custodian**

“Data Custodian” means an internal University service (eg, IT Services), team, or individual to which records or data are entrusted on behalf of the Data Controller (the University) or a Data Owner for the purposes of storage and/or processing.

### **Data Processor**

“Data Processor” means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his or her employment. This includes, eg, service providers storing or hosting records or data.

Data Processors, as external third parties processing University records and data, are subject to the University’s Data Protection Policy and Data Hosting Policies, and to data protection legislation.

### **Staff**

“Staff” means all full-time and part-time employees of the University, staff funded externally but under contract to the University, including seconded staff, and researchers under contract to the University.

### **Students**

“Students” means all full-time and part-time registered students of the University.

### **Other Users**

“Other Users” covers third parties (all the University’s subsidiary companies, contractors, service providers, visitors and/or any other parties) who process records created in the course of the University’s activities, parties to whom such data is disclosed (recipients), and all persons who are granted access to the University’s IT Resources.

## All Users

“All Users” covers Staff, Students, and Other Users, as defined above.

## Records Retention Schedule (“RRS”)

Control document that defines the length of retention and the disposition actions that are authorised for specified records, grouped into records series. The University’s retention schedules include a business classification scheme, linking records to the context of their creation, and other supporting information, including the Data Owner and access classification for each records series.

## 10 Appendix: Data Owners Table

The Data Owner for each records series is set out in records retention schedules. The present table outlines in general terms the Data Owner for the main categories of records and data held.

Functional Area	Data Owner
Academic and Student Administration	Deputy President and Registrar
Academic Governance	DP-Registrar / Heads of Colleges, Schools, Depts
Buildings, Estates, and Facilities Management	Director of Buildings and Estates
Corporate and Legal Administration	Corporate Secretary
Development and Alumni Relations	President
External Relations and Communications	Vice President for External Relations
Finance	Bursar/Chief Finance Officer
Human Resources	Director of Human Resources
Information Services	Librarian and Director of Information Services
Research Support Services	Vice President for Research and Innovation
Teaching and Learning Support Services	Vice President for Learning and Teaching
University Governance	Corporate Secretary

## 11 History and Approval

### Revision History

<b>Date of this revision:</b>	<b>Date of next review:</b>
-------------------------------	-----------------------------

Version Number/Revision Number	Revision Date	Summary of Changes
0.1	March 2004	First adoption of policy by Governing Body
0.2	October 2012	Revised format of policy in line with IT policy framework. Revised policy to include relevant changes
0.3	June 2013	Re-wording and addition of relevant links to IT policy documents
1.0	2018	DRM Project policy review process, to address requirements for management of digital records, data, and systems

### Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
0.2	Oct 2012		Review of section 3 Ownership of Records in consultation with University Solicitor, Hilda O’Keeffe
0.3	June 2013		Review of document by Nora Geary, Deputy Corporate Secretary
1.0	2018		Sub-group of DRM Steering Group have reviewed working drafts of policy

### Approval

This document requires the following approvals:

Name	Title	Date
Nora Geary	Corporate Secretary	2018
UMT	University Management Team (Operations)	2018

This policy shall be reviewed regularly by the University Archivist in light of any legislative or other relevant developments.