Ollscoil na Gaillimhe
University of Galway

Code: **QA 442**
Title: **Record Retention Policy**
Date: **4 October 2022**
Approval: **UMT**

1 Introduction

1.1 Record retention is a collaborative ongoing process requiring the support and active participation of management and employees in design, implementation, compliance, and review.

1.2 University records serve as evidence of functions executed and activities performed and comprises a vital source of knowledge regarding how and why decisions were taken.

1.3 This Policy aims to provide guidance and direction to all University management and staff in relation to record retention and ultimately disposal.

2 Scope

2.1 All records created and received in the course of its official business constitute the official records of University of Galway.

2.2 This Policy applies equally to records created and preserved in electronic and paper formats.

2.3 This Policy applies to all areas and locations of the University and includes all departments, offices, units, research centres and areas of work which form part of the University.

2.4 It is the responsibility of all staff, students, contractors or any other person or entity handling University records in to familiarise themselves with this and all associated policies.

3 Purpose and Objectives

3.1 The purpose of this Record Retention Policy is to ensure University record retention processes are capable of supporting the University's functions and activities, and are compliant with legal, taxation, data protection and privacy regulations, and ensure accountability for as long as is required.

3.2 The objectives of this Policy are to:

- support record retention within the University;
- support the University's administrative and operational requirements, including adherence to University policies and compliance with relevant legislation;
- ensure preservation of records of permanent value and to ensure continued access to appropriate historical records;
- ensure timely destruction of records that no longer need to be retained;
- recognise 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.

4 Definition of a Record

4.1 Records are documents in all formats, which are created/received and maintained as evidence of University business completed or as a source of knowledge and which must be retained for as long as required to meet legal, administrative, financial, operational or historic needs of the University.

4.2 Records may exist in a variety of physical forms including:

- paper documents (written or printed matter);
- electronic records (i.e. word processing files, databases, spreadsheet files, emails, CCTV footage, electronic data on any media etc.);
- books, drawings and photographs;
- anything on which information is recorded or stored by graphic, electronic or mechanical means;
- copies of original records.

5 Role of University Units and Employees

5.1 The University operates a hierarchical system of management whereby responsibility for many of its functions and operations are devolved from Údarás na hOllscoile (Governing Authority) to the University Management Team and ultimately to heads of academic, research, project principal investigators and administrative support units.

5.2 Operational responsibility for the implementation of this Policy rests with the heads of each academic/research/ project principal investigators/ administrative area and support units.

5.3 Various University employees are in possession and control of documentation and records relevant to their functions and as such are considered 'Owners' of same. Owners are responsible for the management and retention of such documentation and records. Examples of documentation and record 'Data Owners' include: -

Data Owner:	**Documentation and Records:**
Buildings Office	Property Title and other Deeds
Library	Library Records
Human Resources Office	Employment Records
Financial Accounting Office	Payroll, Non-Pay and Income Records
Procurement & Contracts Office	Centralised Tender Application and Awards
Health & Safety Office	H & S Records
Research Accounting Office	Scholarships and Research Cost Statements
Office of Vice-President for Research	Research Applications, Funder Contracts, Patent & IP Records
Office of Corporate & Legal Affairs	Legal and Governance Records
Academic Secretary	Academic Records
ISS	Centralised IT and Electronic Records
Principal Investigators	Project records

5.4 Where records are used by more than one department/office/unit, clarity about which office has primary/final responsibility for management of the records should be established between the relevant offices.

5.5 The confidentiality of information within records must be safeguarded at all times. It is the responsibility of each department/office/unit to ensure that the appropriate security measures are observed for maintaining records containing personal or other confidential information.

5.6 Once records have been retained by the creating offices (*in situ* or offsite storage) for the requisite time as stipulated in the unit applicable Record Retention schedule, they must be destroyed or archived for permanent retention as set out in the schedule.

5.7 When scheduled for destruction, records must be shredded, pulped or otherwise disposed of securely. The manner of destruction of records must be appropriate to the level of confidentiality of the records.

5.8 In the case of in-house destruction, the department/office/unit should document and retain the date and manner of destruction of records

5.9 In the case of third-party destruction, a confirmation of destruction should be obtained and retained as proof of destruction. Where administration for the contract is centralised or otherwise done outside of the unit (e.g. University wide contracts for confidential shredding services), the unit should coordinate with the contract administrator as regards keeping an adequate audit trail.

6 Record Retention Schedule

6.1 The University Record Retention Schedule(s) set out a: -
(A) list of the main records held by the University in each unit area; and
(B) their retention period; and
(C) methods of disposal.

6.2 A Record Retention Schedule for each applicable area shall be developed by the Data Owner in conjunction with the University Data Protection Officer.

6.3 Once developed for each academic/research/ project principal investigators/ administrative area and support unit, the Record Retention Schedule will be signed off by the responsible UMT member and will thereafter be published where required and appropriate.

6.4 Each Record Retention Schedule shall be based on administrative and operational best practice, historical significance, University Statutes, policies and legal requirements. Legislation which has particular relevance for this schedule includes but is not limited to the below:

- Universities Act 1997(as may be amended);
- Health, Safety and Welfare at Work Act 2005(as may be amended);
- Freedom of Information Act 2014(as may be amended);
- Data Protection Acts 1988 to 2018(as may be amended);
- General Data Protection Regulation (GDPR) 2016/679.

6.5 The Record Retention Schedule(s) prescribe guidelines for the minimum retention period for a range of records held by the University. However, where there exists a business reason for keeping records for shorter or longer periods, the Data Owner, Head of School or Unit or Principal Investigator should do so and record the reason for same in the template at **Appendix 1** for data

and record retention in order to provide for amendments to the schedule going forward. A copy of this completed template should be provided to the University Data Protection Officer.

6.6 To ensure compliance with the Data Protection Acts 1988 to 2018 (as may be amended) and GDPR, any office which intends to hold records which contain personal data for longer periods than those set out in this schedule should consult the Data Protection Officer to ensure that reasonable justification exists for their retention.

6.7 The Record Retention Schedule(s) should be referred to by all schools or units when reviewing their implementation of this Policy. Where a record could fall under two or more categories, the longer term of retention should normally be chosen.

6.8 The retention periods for documents relating to research projects and capital projects can often be longer than the standard requirement and can apply to all documentation relating to a project. As such, administrators should be attentive to any such contractual retention periods which may be relevant to the records which come through their office.

7 Electronic Records

7.1 In the case of electronic records where the computer equipment is maintained by the University's Information Solutions and Services (ISS), the office which creates/maintains these records must formally agree backup and recovery procedures with ISS (as provided for in the "IT Asset Owner Policy" QA407). This is to ensure that there is no ambiguity as to which office is responsible for records in the event of hardware failure or accidental deletion of records.

7.2 Where electronic records are kept on systems not maintained by ISS, a formal inventory of such records must be maintained by the head of academic/administrative area.

7.3 Staff are reminded that electronic records should be classified in accordance with the University's Data Classification Policy (QA402) and should be handled (stored, transferred, accessed) in accordance with the University's Data Handling Policy (QA401). Staff should ensure that they are familiar with these policies and other applicable ISS policies and procedures, as this Retention Policy is to be read in conjunction with same.

8 Personal Data and Employment Related Records

8.1 A large amount of the records kept by the University contain "Personal Data", as defined under data protection legislation. Personal data is any and all data relating to a living individual, who is or can be identified either from the data or from the data in conjunction with other information. Data protection legislation, including the General Data Protection Regulation (GDPR) and the Data Protection Acts 1988 to 2018 (as may be amended) place particular responsibilities on "Data Controllers" and "Data Processors" when handling Personal Data. It is imperative that the University meets its obligations when performing these roles.

8.2 Records kept regarding a person's employment will contain Personal Data and will often contain what is regarded as "Special Categories of Personal Data". Individual employment files and employment related documentation must be handled with absolute care. Any breach of confidence regarding this type of information can have very serious consequences for the individual concerned, as well as lead to liabilities on behalf of the University.

8.3 The University's policy regarding the handling of personal data and sensitive personal data is set out fully in the Data Protection Policy (QA400). Records which contain personal data must be

retained and handled in accordance with this Policy. Please contact the Data Protection Officer for guidance should you be unsure as to whether the records you hold, or intend to hold, contain personal data and/or if the procedures you have in place regarding their retention are adequate.

9 Responsibilities

Name	**Responsibility**
UMT	Policy Owner Responsible for reviewing and approving this Policy as recommended by the COO and Data Protection Officer. Each UMT member is responsible for signing off on the Record Retention Schedule in her/his area of responsibility as applicable.
Data Owners	Each Unit or School Head or Project Principal Investigator is a Data Owner of the records under their control. Ensuring implementation of Policy. Working with Data Protection Officer on development of Record Retention Schedules for the records under their control. Keeping written records of retention periods where such periods are in conflict with the Record Retention Schedule. Liaising with the Data Protection Officer as required. Seeking training if required.
Internal Audit	Monitoring and reporting compliance with the Policy
Chief Operating Officer	Ensuring that this Policy is reviewed and approved by the UMT as appropriate and liaising with the UMT as appropriate.
Data Protection Officer	Initiate regular reviews of Policy and procedures and ensure documentation is updated as appropriate. Organise targeted training and briefing sessions for University staff as required; Provide advice and guidance to University staff on data protection matters arising from records held. Maintain the University Record Retention Schedule(s) updating where necessary in consultation with the Data Owners. Work with Data Owners on the development of Record Retention Schedules. Work with relevant UMT members for sign off of Record Retention Schedule for her/his area of responsibility.

All employees, and academic areas/units engaged in storing records.	Compliance with Policy

10 Related Documents

University Record Retention Schedule(s)
QA400 Data Protection Policy
QA402 Data Classification Policy
QA401 Data Handling Policy
ISS Policies and Procedures

Appendix 1

Name of office/unit responsible _____ Records Retention Schedule

Class/category of records & documents held in unit/area	Retention period (reason for retention period)	**Final disposition (**After the retention period expires the records should be archived or shredded.)

Prepared by _____Date_____

block capitals & signature

Reviewed By_____Date_____

block capitals & signature