NATIONAL COLLEGE OF IRELAND
DATA RETENTION POLICY

April, 2022

Document Information

Prepared By:	Niamh Scannell	**Document Version No:**	0.1
Title:	Research Data Retention Policy	**Document Version Date:**	06/04/2022
Reviewed By:	National College of Ireland	**Review Date:**	

Distribution List

To	Action	Due Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description
0.1	06/04/2022	Niamh Scannell	Initial Document Created
0.2	03/05/2022	Meera Oke (Chair of the Ethics Committee and Niamh Scannell	Meera Oke suggested alterations and Niamh Scannell made amendments

***Enter document details in the in the tables above and make sure to update as changes are made**

CONTENTS

1 INTRODUCTION

In line with data protection requirements and good information management practices, NCI wish to put in place, and be able to demonstrate, appropriate and effective management of personal and non-personal data collected during the course of research activities.

The implementation of an approved Research Data Retention Policy goes towards demonstrating NCI's commitment to the protection of personal data, and provides a basis for maintaining and improving compliance with data protection requirements and good information management practices.

1.1 PURPOSE OF THIS DOCUMENT

The purpose of this policy is to ensure that personal and non-personal data is properly managed and is stored for no longer than is necessary.

This policy outlines the required data retention periods along with the justification for retention. It also sets out actions to be taken when the retention period expires. It applies to all research data regardless of the media on which it is stored (paper-based, electronic, or otherwise).

In addition, this policy helps ensure that NCI is maintaining the necessary personal data for an appropriate length of time, based on legal and business requirements, and in line with the GDPR 'storage limitation' principle.

1.2. SCOPE AND CONTRAINTS

This document applies to both personal and non-personal data that is collected, used, created, and maintained, in the course of research activities. It applies to this data regardless of the media on which it is stored (paper, electronic, or otherwise).

This policy applies to principles investigators, staff carrying out research while employed by NCI, and individuals who are employed or volunteer to carry out research on behalf of NCI. It is also to provide assistance to Programme Directors, Supervisors, Schools, and Heads of Departments in applying retention and disposal actions to undergraduate research projects, postgraduate research projects, and departmental research projects.

All retention periods must be reviewed and updated in line with legal, regulatory, and business requirements.

1.3. POLICY REVIEW, APPROVAL, AND CONTINUOUS IMPROVEMENT

In line with best practice, this policy has been approved by senior management, along with a commitment of continual improvement. This document will be reviewed at least annually by senior management, the Research Committee, the Ethics Committee, and the NCI Data Protection Officer to ensure alignment with changing business and legal requirements.

1.4. ROLES AND RESPONSIBILITIES

All staff, contractors, and volunteers are responsible for ensuring compliance with NCI's research data retention requirements, and obligations. It is the responsibility of all individuals carrying out research on behalf of NCI to ensure:

1. They are familiar with this policy and related relevant policies
2. They complete the mandatory data protection training and research data management training
3. Queries in relation to research data management are promptly and courteously dealt with. When an employee receives an enquiry about the retention of research data, they must know what to do and or/where to refer the request to.

Line Managers, Heads of Functions or Departments, or Business Owners are responsible for ensuring that their department is in compliance with this policy. When the retention period of the record has expired, they shall ensure that the record is maintained, destroyed, or archived in line with the requirements set out in this document.

1.5 REFERENCES

- Research Data Management Policy
- Data Protection Policy
- Personal Data Risk Classification Scheme
- Data Governance Classification and Handling Policy
- Bring Your Own Device Policy
- Portable Storage Device Policy
- General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2014

2 Data Retention Considerations

The following items must be considered when determining the retention period for records and data concerning research:

1. If personal data is being processed, the legal basis for processing must be defined and known. Specifically, if there is no legal basis for processing of the personal data, it must be destroyed and must not be retained. It is not valid to retain information "just in case" it may be required in the future.
2. In some instances, statutory or regulatory requirements may apply. For example, Revenue requirements for retaining of financial records. In these scenarios, the retention periods are fixed for compliance with a legal obligation to which NCI are subject and therefore must comply. This requirement will take precedence in defining the retention periods.
3. In some instances, funding bodies may stipulate a period for which specific records and information are to be retained. This requirement will be taken into account and applied to relevant records.
4. If personal data is being processed and there is valid lawful basis for processing, yet no legal requirements, a decision must be made considering the 'storage limitation' principle. Specifically, a balancing test is required between business need versus the nature, scope, context and purposes of the processing, and whether it is likely to result in a high risk to the rights and freedoms of natural persons.
5. NCI shall avoid accommodating every conceivable need for retaining personal data, however it may make sense that certain attributes of personal data are destroyed while other attributes are retained due to legal or business requirements.
6. Where information is required to be retained for reporting or analytical purposes, the information must be anonymised in such a manner that the data subject is no longer identifiable. In this instance, the information is no longer considered personal data.

7. Where research participants have been informed that their data will not be further analysed, shared with other researchers/institutions, and/or only held for a specific amount of time, it is most likely that participants will be required re-consent if stated practices are to change.

Records containing personal data shall always be destroyed or archived in a secure manner once the retention period has expired. This includes the following:

1. Paper records requiring destruction shall be shredded in line with best practice, and where this is done in-house, a record of the date and manner of destruction must be maintained. The record must specifically maintain the date and manner of destruction of records which are identified for destruction following the expiry of the retention period. Documents containing personal data which may be printed and shredded as part of the day-to-day work of the organisation do not need to be included on the record unless it contains special categories of data, and the loss of the document may result in a high risk to the rights and freedoms of the individual. A record destruction schedule template is included in Appendix A.
2. Where possible, locked paper bins should be provided and located in areas easily accessible to staff. When paper is collected from the bins for shredding, the date of destruction must be recorded. Where a third-party performs the destruction, certificates or other form of confirmation of destruction shall be obtained as evidence of secure destruction. The latter certificates are currently held by the DPO.
3. Where paper records must be archived, consideration shall be given to where the archives will be stored, under what conditions they will be stored, retrieval procedures, how the archive data will be recorded and tracked, and who is authorised to access the archived data.
4. Storage of archived data must be secure and appropriate to the risks associated with the storage of the data, as well as in line with the requirement to fulfil data subject access requests i.e. it must be possible to respond to a data subject access request within the required timeframe.
5. Research data, in particular records and documents that contain personal data, stored digitally must be securely erased or destroyed using best practice methods. Where a third-party performs the destruction, certificates of destruction shall be obtained, and these shall be maintained as evidence of secure disposal of the data. Where done in-house, any removable media such as USBs, backup media, decommissioned smartphones, etc. containing data must be physically destroyed or shredded so that data cannot be retrieved from the device. A record of the date and manner of destruction must be maintained.
6. Where personal data is archived in a digital format, consideration shall be given to the format and method of storage so as to ensure that it can be retrieved and read at a future date. The Research Data Management Policy provides guidance on this matter.
7. The risks associated with the method of digital storage must be assessed, and the required technical and organisational controls shall be implemented to ensure that archived digital data is kept secure for the required duration. The Research Data Management Policy provides guidance on this matter.

3 LITIGATION HOLD

3.1 WHAT IS LITIGATION HOLD

NCI requires all NCI staff and employees to fully comply with the general guidance set out in this policy and the specific retention periods it sets out. However, all NCI staff and

employees should note the following general exception to any stated destruction schedule:

if you believe, or the NCI DPO and/or the HR Department informs you, that certain data held by NCI is relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit or other event, you must preserve and not delete, dispose, destroy or change such data, including e-mails, until NCI DPO and/or HR determines that such data is no longer needed. This exception is referred to as a "Litigation Hold", and takes priority over any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact the NCI DPO and/or the HR Department.

3.2. WHAT TO DO WHEN NOTIFIED OF A LIGITGATION HOLD

The destruction of Data must stop immediately upon notification from NCI DPO and/or the HR Department that a litigation hold is to begin due to ongoing or potential litigation or an official investigation. Destruction may begin again once NCI DPO and/or the HR Department, as appropriate, has confirmed that the relevant litigation hold has been lifted.

Research Data Retention Schedule

Data Type	Business Retention Period	Justification	Guidance	Expiry Action
Applications to the Ethics Committee	5 years or per funding body requirements	In compliance with the Ethics Committee requirements to allow research findings to be contested or audited or facilitate civil claims that may arise.		Confidential shredding and/or secure deletion of electronic records.
Research data and findings (notes, interview transcripts, statistical records)	5 years or per funding body requirements	In compliance with the NCI Ethics Application Agreement to allow research findings to be contested or audited or facilitate civil claims that may arise.		Confidential shredding and/or secure deletion of electronic records.
Financial records associated with research projects	7 years or per funding body requirements	Section 285 of the Companies Act 2014 states that accounting records are to be kept for at least 6 years after the end of the financial year. Section 886 of the Taxes Consolidation Act 1997 states records are to be kept for a minimum of 6 years after the completion of the transactions, acts, or operations to which they relate. Records held beyond the 7 year period are to meet funding body requirements.	Single official record to be held by designated office holder, with access available to all authorised officers. Duplicates to be destroyed/deleted as soon as feasible	Confidential shredding and/or secure deletion of electronic records.
Contracts and agreements	7 years or per funding body requirements	Section 11 of the Statute of Limitations 1957 provides a limitation period of 6 years for perceived breaches of contracts to be addressed by law. The 7 year period allows for claims which may be commenced towards the end of the limitation period. Records held beyond the 7 year period are to meet funding body requirements.	Single official record to be held by designated office holder, with access available to all authorised officers. Duplicates to be destroyed/deleted as soon as feasible	Confidential shredding and/or secure deletion of electronic records.
Postgraduate Research Student Files (application forms, proposals, progress reports,	Retain for duration of studies plus 5 years? or per funding body requirements	Article 90 of Council Regulation (EC) No. 1083/2006 requires		Confidential shredding and/or secure deletion of electronic records.

examiner reports, external reviews, stipend payments, etc.)		records for the 2007-2013 period to be held until 2022 Article 140 of Council Regulation (EC) No. 1303/2013 requires records for for the 2014-2020 period to be held until 2029		
Postgraduate Theses	Permanent	Part of the College record		Retained in the Library.
Contractor and volunteer records	7 years after employment ceases	Section 11 of the Statute of Limitations 1957 provides a limitation period of 6 years for perceived breaches of contracts to be addressed by law. The 7 year period allows for claims which may be commenced towards the end of the limitation period.	Single official record to be held by designated office holder, with access available to all authorised officers. Duplicates to be destroyed/deleted as soon as feasible	Confidential shredding and/or secure deletion of electronic records.

Appendix A: Records Destruction Schedule

Name	
Department/Function	
Head of Department/Function	

Description of records	Retention period	Date range	Media (paper, electronic, etc.)	Date of Destruction	Method of Destruction	Authorisation of Disposal

Appendix B: Log-in Instructions for Data Protection Training

Accessing Legal Island GDPR Staff Training

All staff must complete the online training modules. Each will take a maximum of around 55 minutes. Many of you will complete the training in less than this time. Instructions as to how to log on are shown below.

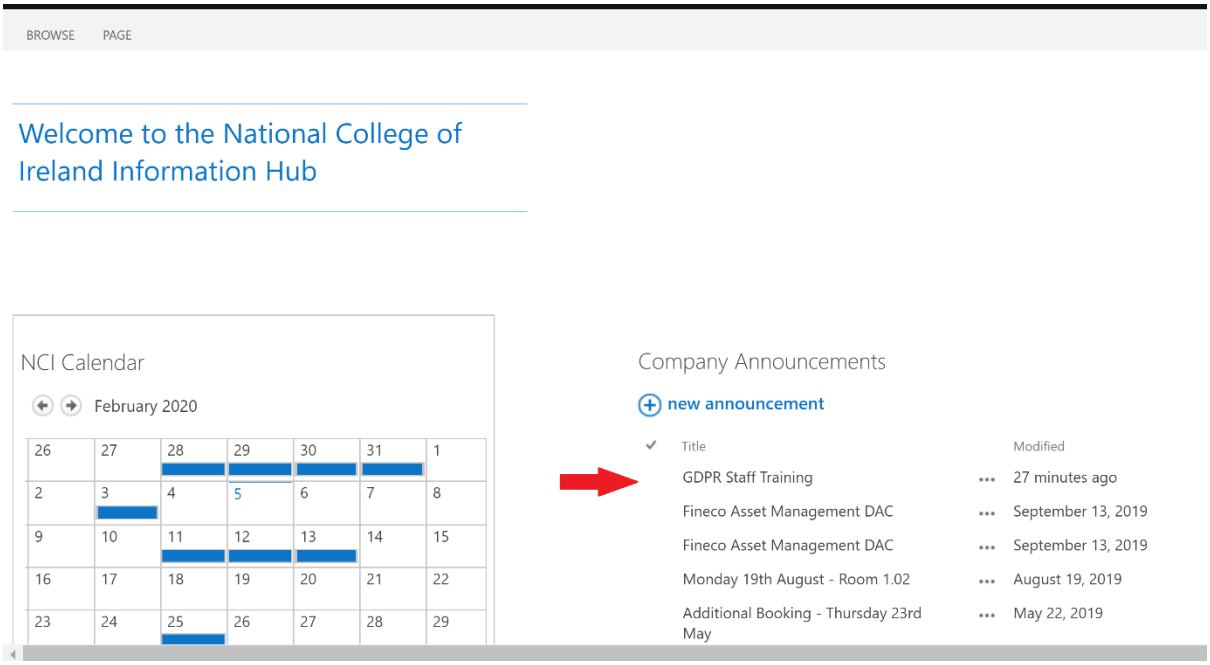
Please ensure that you have completed all modules and save/print the certificate at the end. The College is legally required to maintain records of staff training and the Legal Island system will record your training as long as you complete all the required steps.

1. **Access to the Legal Island System**

To access the Legal Island system, please go to this link and select National College of Ireland

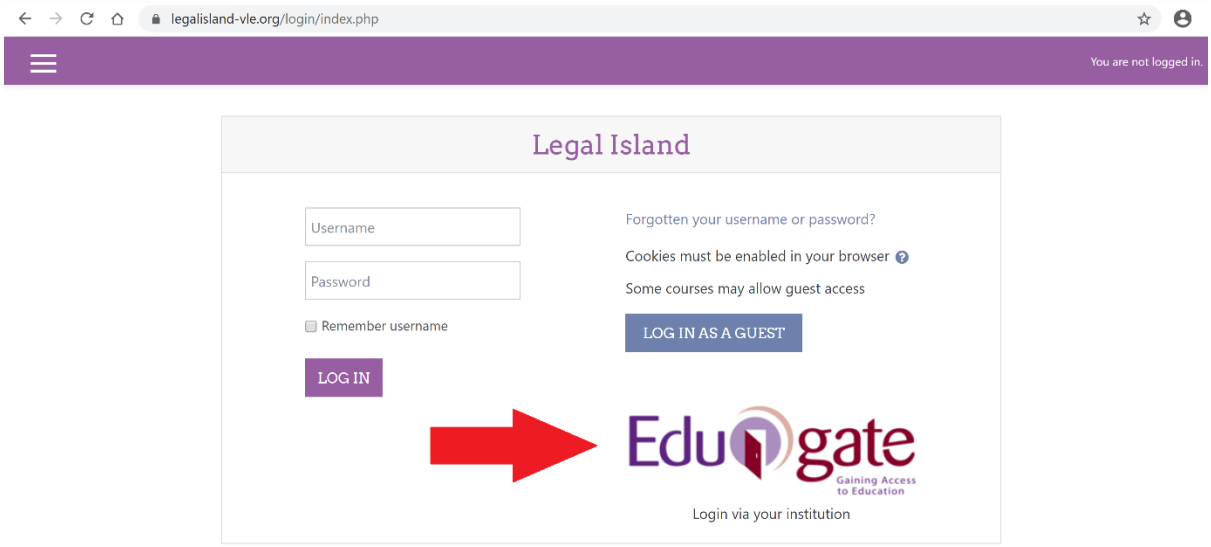
OR

You can access the Legal Island system through the NCI Information Hub as shown below



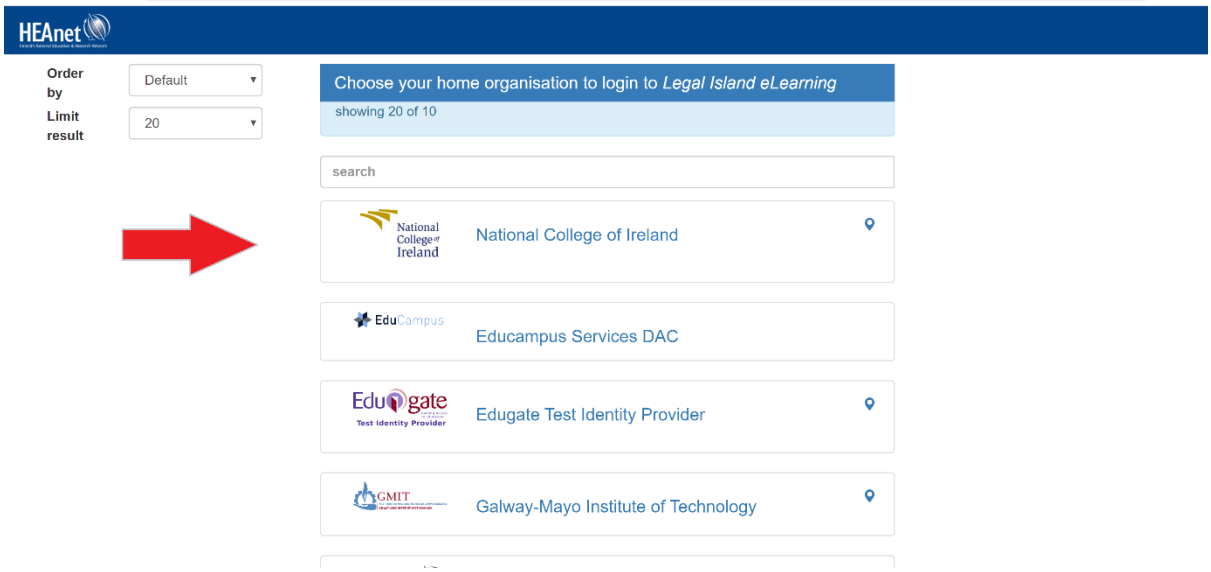
2. **Educate Log-In**

You will be brought to the page below. Click on Edugate to log in



3. Selecting National College of Ireland

Select the National College of Ireland as shown below



4. Logging In

Many of you will be automatically logged in. If you are not, enter your user name and password

Please note that your user name ***does not*** include your @staff.ncirl.ie extension

5. Courses to Complete

If you have not done Legal Island training before, please complete the modules available