lyit | Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Data Retention Policy

June 2018

Contents

Revision History

Date of this revision: 21/6/2018	Date of next review: 21/6/2019

Document Location

Website – Policies and Procedures	x
Website – Staff Hub	x
Website – Student Hub	
Other:	

Approval

This document requires the following approvals:

Name	Title	Date
HMG	Executive Board	11 June 2018
HMG	Governing Body	21 June 2018

This Policy was agreed by the Governing Body on 21 June 2018. It shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

1. OVERVIEW

The Institute is responsible for the processing of a significant volume of information across each of its Schools and Department. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

- It is the responsibility of each School and Function to ensure this information is processed in a manner compliant with the relevant data protection legislation and guidance.
- The Institute has an appointed Data Protection Officer (DPO) who is available to Schools and Functions to provide guidance and advice pertaining to this requirement.
- All Staff must appropriately protect and handle information in accordance with the information's classification.
- Confidential Information requires the greatest protection level (e.g. personal data).

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

2. PURPOSE

The purpose of this policy is to ensure that the Institute applies retention periods appropriately and retains data only for the period for which it is allowed under these new retention periods. It sets out the procedures that should be in place and puts responsibility on each School and Function to ensure that the Institute remains compliant with this area of the regulation.

3. SCOPE

This policy applies to:

- Any person who is employed by LYIT who receives, handles or processes data in the course of their employment.
- Any student of LYIT who receives, handles, or processes data in the course of their studies for administrative, research or any other purpose.
- Third party companies (data processors) that receive, handle, or process data on behalf of LYIT.

4. POLICY

This policy should not be viewed in isolation. Rather, it should be considered as part of the LYIT's suite of Data Protection policies and procedures (see Appendix A).

Institute policy is to retain and dispose of information in compliance with legal and regulatory requirements together with this Data Retention Policy and related policies. In particular:

- Data Protection legislation only applies to a living individual's personal information, e.g. student or staff information (potential, current or past). Commercial requirements may drive disposal of other information, not covered by Data Protection.
- Data Protection legislation cannot override other legislation or regulations defining personal information minimum retention requirements. However, Schools and Functions must confirm which retention requirement defines appropriate retention periods.
- This document only deals with those parts of Data Protection Legislation, which relate to information retention, disposal and retrieval.

4.1 Information Retention and Disposal Policy

Schools and Departments must define appropriate Management Processes to comply with information management policy, legal and regulatory requirements, international standards, and best practices.

These processes must:

- Be based on the information owner's approval of these information use processes.
- Be sufficiently flexible to cope with temporary changes to retention requirements for example if information is required for investigations or potential litigation.
- Be cognisant of other department's dependence on any retained or disposed information.
- Use appropriate security requirements based on School and Function information classification levels as laid out in the Information Security Policy.
- Include appropriate retention mechanisms facilitating reasonable retrieval times to support Institute business, regulatory or disposal requirements.
  Use and maintain appropriate and durable information retention/retrieval mechanisms to prevent damage, degradation or unauthorised alteration and ensure retrieval at any time.

Schools, Functions and Information Owners must develop, maintain, procure and manage information retention and disposal procedures, mechanisms, facilities and services to ensure that they are effective.

Each School/Function and Information Owners must manage the information, including assessment, storage, retrieval and disposal in accordance with this policy and related policies in order to ensure that the information is retained for the appropriate period of time, in a manner which befits its sensitivity and value.

Schools and Functions shall also ensure that all retained information, within their area of responsibility is:

- Identified, recorded, and assessed to ensure that it is appropriately managed throughout the retention and disposal life-cycle.
- Subject to appropriate information management procedures throughout the retention and disposal life cycle.
- Subject to periodic procedure effectiveness reviews.

Schools and Functions must also:

- Communicate all changes to relevant parties.
- Ensure that all students, staff, vendors, independent contractors, consultants and other LYIT's IT resource users, charged with managing retained information, are familiar with and trained on all relevant procedures aware of their responsibilities.
- Provide timely notification to students, staff, vendors, independent contractors, consultants or entities that use LYIT's IT resources, when information is required to be retrieved, e.g. to support investigations or litigation, to prevent this information from being destroyed.
- Retrospectively assess existing information, stored prior to this policy implementation to ensure appropriate documentation, management and disposal.
- Report any inability to comply with this policy via the regular Risk Management processes.

Each School and Function must complete Data Process Inventory, documenting all information categories required for retention within its responsibility. In particular:

- Establish appropriate retention requirements for each category.
- Review and update this inventory regularly or post significant change introduction.

Schools and Functions must refer all retention period ambiguities to the DPO and/or Legal Services prior to information disposal. When deciding upon an acceptable retention period, the decision should be grounded on an appropriate legal basis. Schools and Functions should seek to reduce retention periods as much as possible.

Schools and Functions must contractually ensure that all Contractors and external service providers manage information retention services in such a manner as to:

- Minimise risk to the Institute, its employees and its (potential, past, or current) students.
- Ensure that contractors or external service providers allow reasonable audits and inspections access.
- Include, as a minimum, provisions for non-compliance with defined policies and standards, malicious or negligent activities by their employees or agents, and termination of agreement.
- Ensure that Institute information and related records, on which the Institute is reliant, are available and appropriately protected until the period of reliance has elapsed.

Schools and Functions must report non-compliance instances to the:

- DPO
- Person responsible for a School/Function.

4.2 IT Role and Responsibilities

IT shall:

- Review and provide policy input and relevant related documentation, e.g. IT, policies, standards and guidelines.
- Ensure that the technical aspects of the information retention and disposal requirements, as defined by the Information Owner are met, including monitoring of the service provided.
- Support the Information Owner or their representative with those aspects of the Data Retention Schedule which relate to electronic information.
- Ensure that all copies made of information, within the scope of this policy, whether for development or test purposes, or for internal or external use, are subject to, as a minimum, the same controls as the original information.
- Manage Institute information, in compliance this policy and related standards.
- Monitor the supporting processes to ensure ongoing compliance.
- Notify the Information Owner or his/her nominated representative of any non-compliance discovered.
- Ensure that staff or agents acting on their behalf are fully familiar with and trained on all of the relevant policies and procedures and that they are aware of their responsibilities.
- Provide supporting evidence of compliance on request to the Information Owner and DPO.
- Allow appropriate access to the Information Owner or their appointed representatives.

4.3 DPO Roles and Responsibilities

The DPO shall:

- Establish and maintain effective policies, standards and guidelines relevant to information retention and disposal.
- Distribute relevant documents to Schools and Functions including policy or related standards/guidelines updates.
- Periodically review all relevant policies and related standards/guidelines for effectiveness.
- Provide relevant advice and support to Schools and Functions to assist them in achieving and retaining policy/standards compliance.
- Monitor policy and standards compliance and ensure that School and Function plans provide for this compliance.

4.4 Legal Services Roles and Responsibilities

Based on request for the Institute, the Institute-appointed Solicitor shall:

- Review and provide policy input and related documentation, e.g. standards and guidelines.
- Provide information retention and disposal legal advice to Schools and Functions.
- Assist Schools and Functions with contract drafting relating to external service providers providing information retention and disposal services.

4.5 Data Protection Oversight Committee Roles and Responsibilities

The Data Protection Oversight Committee shall:

- Approve any compliance exceptions.
- Handle any breaches in data protection that occur.

5. POLICY COMPLIANCE

5.1 Compliance

Breaches of this policy may result in data breaches under data protection legislation, reputational damage to LYIT and an infringement of the rights of employees or other relevant third parties.

5.2 Compliance Exceptions

Any exception to the policy shall be reported to the Data Protection Officer in advance by email to dpo@lyit.ie.

5.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the Institute's disciplinary procedures. Failure of a third party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

Non-compliance shall be reported to the Data Protection Officer and the Data Protection Oversight Committee.

APPENDIX A: SUPPORTING DOCUMENTS

The below is a list of a suite of policies and procedures that may be used in conjunction with this policy.

- Data Protection Policy
- Data Protection Procedures
- Data Governance Policy
- Information Security Policy
- Network Security Policy
- Systems Development Life Cycle Policy
- Data Access Management Policy
- Data Handling & Clean Desk Policy
- Data Encryption & Data Anonymisation and Pseudonymisation Policy
- Privileged User Policy
- IT Architecture Security Management Policy
- Data Protection Incident Response & Breach Notification Policy.

The above list is not exhaustive and other LYIT policies, procedures and standards and documents may also be relevant.

APPENDIX B: GLOSSARY OF TERMS

Records	Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by LYIT. Examples of personal data include, but are not limited to: • Name, email, address, home phone number • The contents of an individual student file or HR file • A staff appraisal assessment • Details about lecture attendance or course work marks • Notes of personal supervision, including matters of behaviour and discipline.
Data	As used in this Policy shall mean information which either: • is Processed by means of equipment operating automatically in response to instructions given for that purpose • is recorded with the intention that it should be Processed by means of such equipment • is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System • does not fall within any of the above, but forms part of a Readily Accessible record. Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	Means a person or organisation that holds or Processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data. An employee of a Data Controller, or a School or Function within an Institute which is Processing Personal Data for the Institute as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the Processing of Personal Data would be a Data Processor.

	It is possible for one Institute or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether the Institute is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the DPO or Legal team.
Third Party	Means an entity, whether or not affiliated with LYIT that is in a business arrangement with LYIT by contract, or otherwise, that warrants ongoing risk management. These Third Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where <Institute Name> has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to Process Personal Data.

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as the GDPR and/or local requirements.

Institiúid Teicneolaíochta
Leitir Ceanainn
Letterkenny Institute
of Technology

Bóthar an Chalaidh, Leitir Ceanainn
Contae Dhún na nGall, Éire

Port Road, Letterkenny
County Donegal, Ireland

Telephone + 353 74 918 6000
Fax + 353 74 918 6005

www.lyit.ie