

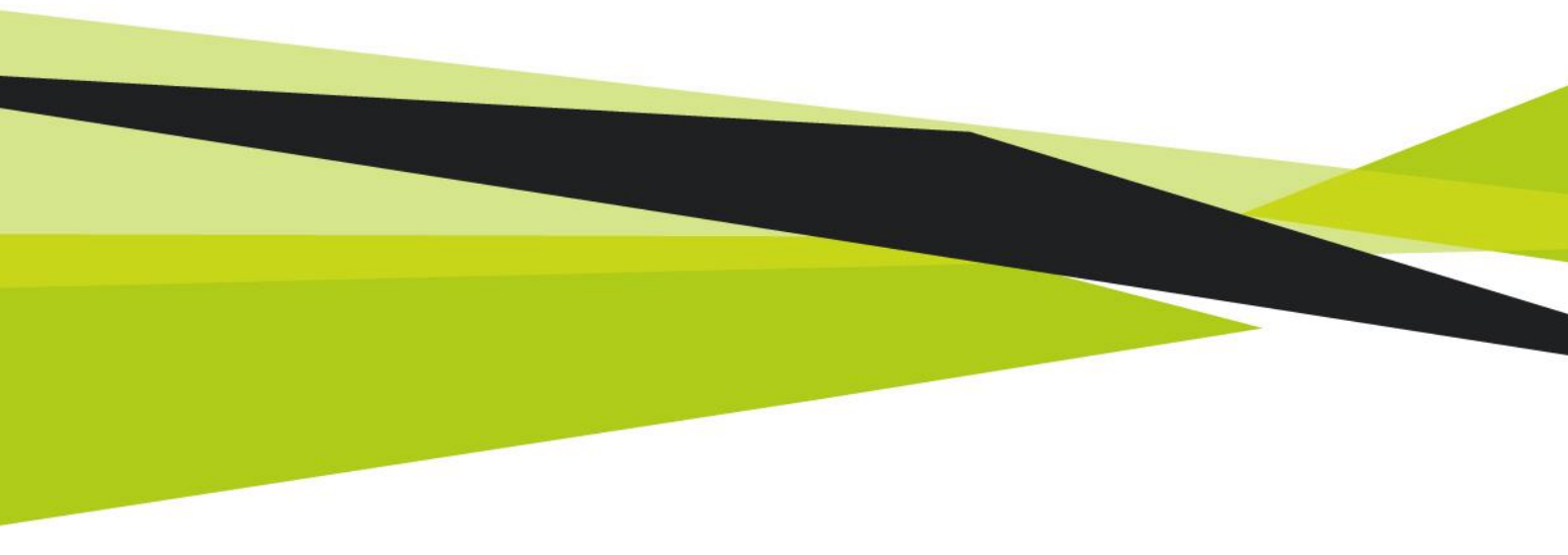


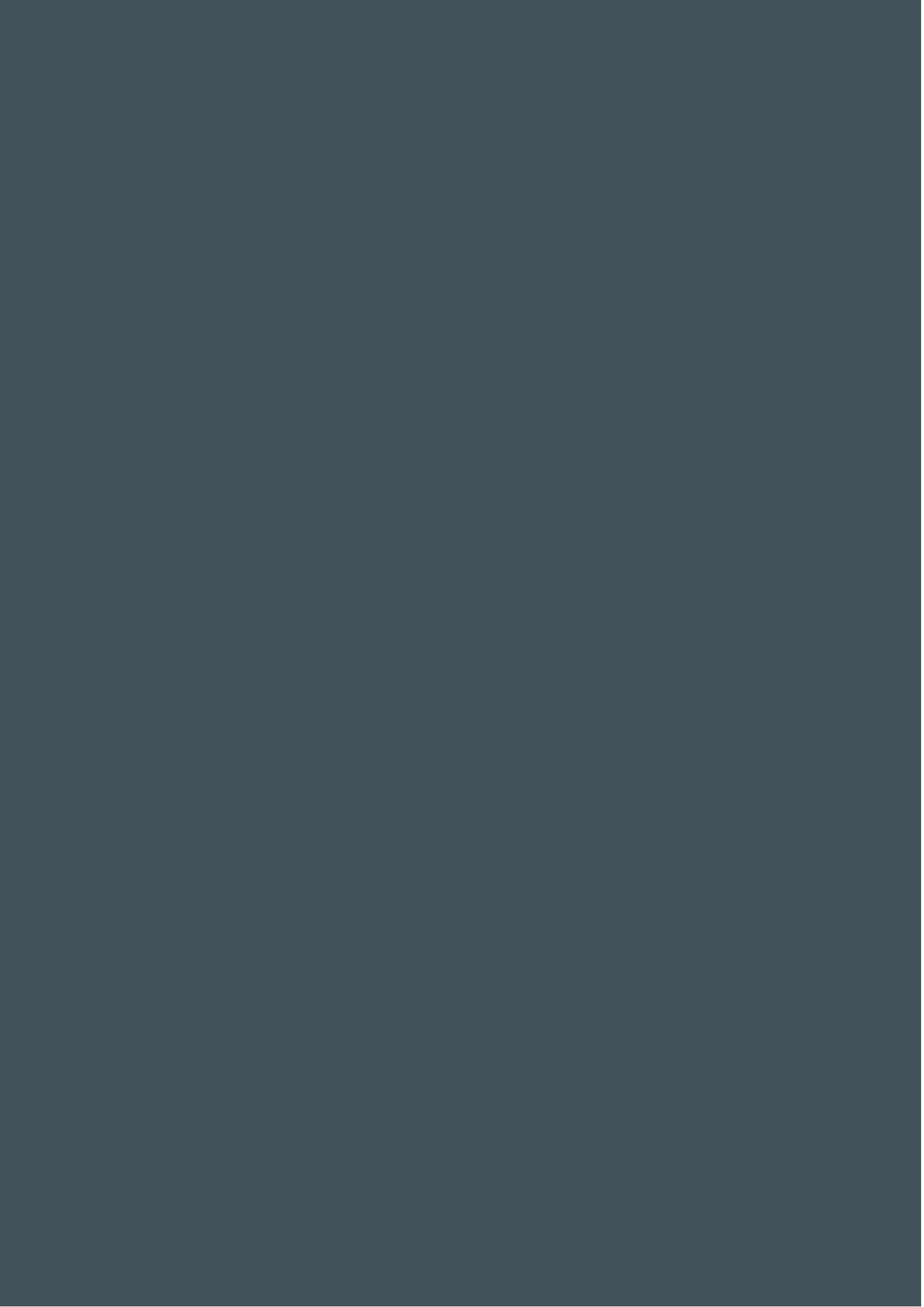
lyit

Institiúid Teicneolaíochta Leitir Ceanáin
Letterkenny Institute of Technology

Data Governance Policy

June 2018





Contents

1.	OVERVIEW.....	1
2.	PURPOSE.....	1
3.	ROLES AND RESPONSIBILITIES	1
4.	SCOPE	2
5.	POLICY.....	3
5.1	Information Governance	3
5.1.1	Data Ownership.....	3
5.1.2	Data Classification.....	4
5.1.3	Retention of Data	6
6.	POLICY COMPLIANCE.....	6
6.1	Compliance.....	6
6.2	Compliance Exceptions.....	6
6.3	Non-Compliance	6
	APPENDIX A: SUPPORTING DOCUMENTS.....	7
	APPENDIX B: DATA REGISTER	8
	APPENDIX C: GLOSSARY OF TERMS.....	9

Revision History

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

Document Location

Website – Policies and Procedures	<input checked="" type="checkbox"/>
Website – Staff Hub	<input checked="" type="checkbox"/>
Website – Student Hub	<input type="checkbox"/>
Other:	<input type="checkbox"/>

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 Departments. 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

To provide direction on the classification, ownership and retention of data and information for LYIT as well as clarifying accountability for data and information. Data and information as pertaining to this policy includes electronic and non-electronic data.

LYIT is reliant upon the confidentiality, integrity, and availability of its data and information to successfully conduct its operations, meet student and staff/faculty expectations, and provide services.

Therefore, all staff, faculty, students, and external parties of LYIT have a responsibility to protect Institute data and information from unauthorised generation, access, modification, disclosure, transmission or destruction and are expected to be familiar with and comply with this policy.

3. ROLES AND RESPONSIBILITIES

The following roles and responsibilities apply in relation to this Policy:

<i>Governing Body</i>	To review and approve the policy on a periodic basis
<i>Executive Board</i>	<p>The Executive Board (EB) is responsible for the internal controls of LYIT an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. The EB is responsible for:</p> <ul style="list-style-type: none">• Reviewing and approving this Policy and any updates to it as recommended by the Office of the Institute Secretary.• Ensuring ongoing compliance with the GDPR in their respective areas of responsibility.

	<ul style="list-style-type: none"> • As part of the Institute’s Annual Statement of Internal Control, signing a statement which provides assurance that their functional area is in compliance with the GDPR. • Ensuring oversight of data protection issues either through their own work or a Data Protection Oversight Committee or other governance arrangement.
<i>Data Protection Officer</i>	<ul style="list-style-type: none"> • To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR. • To advise on all aspects of data protection and privacy obligations. • To monitor and review all aspects of compliance with data protection and privacy obligations. • To act as a representative of data subjects in relation to the processing of their personal data. • To report directly on data protection risk and compliance to executive management.
<i>Staff/Students/External Parties</i>	<ul style="list-style-type: none"> • To adhere to policy statements in this document. • To report suspected breaches of policy to their Head of Department and/or Data Protection Officer.
<i>Data Processor</i>	Management and staff within the LYIT who take responsibility for processing, storing and/or archiving Institute data. Data processors take responsibility to apply the relevant information handling controls required per the classification of data set out in section 5 below.

If you have any queries on the contents of this Policy, please contact the Executive Board or Data Protection Officer via email dpo@lyit.ie.

4. SCOPE

This Data Governance Policy relates to all LYIT’s data including but not limited to:

- LYIT Student Data
- LYIT Staff Data
- LYIT Financial Data
- LYIT Commercial Data
- LYIT Intellectual Property
- Academic Data.

LYIT is committed to ensuring that all LYIT data is clearly identified and an inventory of all important data is drawn up and maintained. The data inventory includes data held on all IT resources and application types including Microsoft (MS) Excel spread sheets, MS Access databases and other such end user application. Appendix B provides a template for the maintenance of a data inventory.

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.

This applies whether you are working in the Institute, travelling or working remotely.

5. 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); in particular please refer to Data Handling & Clean Desk Policy for further information on the minimum requirements for handling data and maintaining a "clean desk".

5.1 Information Governance

5.1.1 Data Ownership

All information and assets associated with information processing facilities (applications) should be owned by a designated part of the organisation. Therefore, data ownership to key sets of information and data (and associated applications) must be formally assigned.

Ownership of data resides with LYIT and implies authority as well as responsibility and control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, but also the right to assign these access privileges to others.

In the context of LYIT data ownership responsibility will be formally assigned for the following functional domains/process but is not limited to these functions:

- HR
- Payroll processes
- Student Administration processes/services
- Information Systems
- Financial processes
- Resource Planning.

Data ownership responsibilities include:

- Approval of user access
- Approval of user roles/profiles/classes
- Review of access including application data held in network directory locations
- Data classification
- Data retention rules and definition
- Master data changes authorisation
- Ensuring availability of information

- Data restoration testing
- Service level management and monitoring.

5.1.2 Data Classification

The purpose of information classification is to ensure that information/data receives an appropriate level of protection.

Following on from this, LYIT classifies its data based on the level of impact that would be caused by inappropriate access and/or data loss. There are three classifications as follows:

<i>Impact Level</i>	<i>Types of Classification</i>
High	Confidential data (+ Strictly Confidential Data)
Medium	Internal Use Only data
Low	Public data

Classification of data is independent of its format. The following table provides an indication of how classifications get assigned through considering the impact of various risks:

Risk	Impact is considered from four main perspectives- legal, reputational, financial, and operational		
Inappropriate access causing breach of confidentiality/data protection rules	Serious	Moderate	Minor
Inappropriate access resulting in unauthorised amendments	Serious	Moderate	Minor
Data loss	Serious	Moderate	Minor
Unauthorised disclosure	Serious	Moderate	Minor

Resulting Data Classification	Confidential Data (+ Strictly Confidential Data)	Internal Use Only	Public Data
Data Classification examples	<ul style="list-style-type: none"> • Finance Data relating to students and personnel • HR Data • Commercially Sensitive Data • Personal Data (under GDPR Legislation) <p><i>Strictly Confidential</i></p> <ul style="list-style-type: none"> • <i>Special Categories of Personal Data (under GDPR Legislation).</i> 	<ul style="list-style-type: none"> • Intranet / Extranet data • Internal telephone books and directories • Financial Budgets 	<ul style="list-style-type: none"> • Public Websites • Campus Maps • Staff Directory

Data that is not yet been classified should be considered **confidential** until the owner assigns the classification.

Confidential Data

Confidential data is information or data protected by statutes, regulations, Institute policies or contractual obligation. Personal data is considered to be **confidential or strictly confidential** data (see distinction above). Prior to the distribution or transmission of confidential data, it is required that reference is made to relevant legislation, (which at this time is the General Data Protection Legislation or GDPR) to ensure such distribution or transmission is not in breach of same. Confidential data should only be disclosed to authorised individuals on a need-to-know basis and in accordance with the relevant legislation. By way of illustration only, some examples of confidential **(C)** and strictly confidential **(SC)** data include:

- Medical records **(SC)**
- Student records and other non-public student data **(C) or (SC)** (see Special Categories of Personal Data under GDPR)
- PPS Numbers **(C)**
- Personnel and payroll records **(C)**
- Bank account numbers and other personal financial information **(C)**
- Financial budgets [Commercially Sensitive – **(C)**].

Confidential data, when stored in an electronic format, must be protected with strong passwords and stored on servers that have appropriate access control measures in order to protect against loss, theft, unauthorised access and unauthorised disclosure.

Confidential data must not be disclosed to parties without explicit management authorisation. Confidential data must only be used for the purpose for which it was originally gathered. If, for legitimate teaching, learning and/or research activities confidential data is used for a purpose other than that of which it was originally gathered the data must be anonymised.

Internal Use Only Data

Internal only data is confidential information that must be protected due to proprietary, ethical, or privacy considerations, and must be protected from unauthorised access, modification, transmission, storage or other use. Internal use data is information that is restricted to members of the LYIT's community who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of official use data include:

- Intranet / Extranet data.
- Internal telephone books and directories.

Internal Use only data must be protected to prevent loss, theft, unauthorised access and/or unauthorised disclosure.

Public Data

Public data is information that may be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data can be made available to all members of the LYIT's community and to all individuals and entities external to the LYIT's community.

By way of illustration only, some examples of public data include:

- Publicly-posted content on all external-facing web sites
- Publicly-posted press release
- Publicly-posted schedules of classes
- Publicly-posed interactive Institute maps, newsletters, newspapers and magazines.

5.1.3 Retention of Data

It is the responsibility of data owners to clearly indicate the maximum period of time information/data should be retained by the Institute.

Please refer to Data Retention Policy for information on retention periods.

6. POLICY COMPLIANCE

6.1 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.

6.2 Compliance Exceptions

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

6.3 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 at dpo@lyit.ie.

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 Retention 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: DATA REGISTER

Note: Please refer to Data Retention Policy for further information on retention periods.

Excel copy available from the DPO via email dpo@lyit.ie.

GDPR Data Processing Register																
LYIT																
Data Controller:		LyIT														
DPO		Frances Wilson														
ARTICLE 30 RECORD OF PROCESSING ACTIVITIES																
Ref	School, Department or Function	Data Processor	Personal Data Processing Activity	Description of the Data Process / procedures	Types of Data Subjects	ARTICLE 14 Sources of where the personal data is collected	Types of non-special categories of Personal Data	ARTICLE 6 Legal basis for the processing of non-special categories of personal data	Types of Special categories of personal data	ARTICLE 9 Legal basis for the processing of Special categories of personal data	Internal sharing of personal data- Categories of recipients receiving the data internally	External transfers of personal data - Categories of recipients who the data is transferred to externally, including cloud based service u	General Description of the Technical and Organisational Security measures/controls, if possible	Location of where the personal data is stored	Records Retention period and review current records retention policy	Actions required to be GDPR compliant / methods of destruction
1																
2																
3																

APPENDIX C: GLOSSARY OF TERMS

<i>Content</i>	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
<i>Records</i>	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.
<i>Metadata</i>	<p>Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include:</p> <ul style="list-style-type: none"> • Title and description, • Tags and categories, • Who created and when, • Who last modified and when, • Who can access or update.
<i>Personal Data</i>	<p>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.</p> <p>Examples of personal data include, but are not limited to:</p> <ul style="list-style-type: none"> • 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.
<i>Sensitive Personal Data</i>	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.
<i>Data</i>	<p>As used in this Policy shall mean information which either:</p> <ul style="list-style-type: none"> • 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.
<i>Data Ownership</i>	A process whereby information/data is assigned an appropriate owner whose roles and responsibilities in relation to that information/data are clearly documented. This is also deemed to include any data of an academic nature. Acknowledge nature of Institute – Refer to information security policy on controls over creation, transmission, storage.
<i>Data Classification</i>	A process whereby information/data is classified in accordance with the impact of data being accessed inappropriately, and/or data being lost. The resulting data classification can be associated with a minimum level of control which then needs to be applied when handling data. It is the responsibility of data owners to classify their data.
<i>Data Controller</i>	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.
<i>Data Processor</i>	<p>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.</p> <p>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.</p>
<i>Third Party</i>	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 LYIT has an ongoing relationship. Third Party

	<p>relationships, for the purposes of this Policy, generally do not include student or customer relationships.</p> <p>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.</p>
<i>Confidential Data</i>	Includes any data covered by GDPR under the category of personal data. This also includes information considered to be commercially sensitive to the Institute. Examples include strategic plans or intellectual property.
<i>Strictly Confidential Data</i>	Data covered by GDPR under the category of sensitive personal data or special categories of personal data. If this data were to be disclosed to an unauthorised party, it could result in the loss of public confidence, non-compliance with regulatory compliance, legal liabilities and/or additional costs. Special categories under GDPR include child data and health data.
<i>Data Subject</i>	Refers to the individual to whom Personal Data held relates, including: employees, students, customers and students.
<i>Encryption</i>	It is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network. Refer to the information Security Policies relating to Information Protection for further Guidance on this area.
<i>Processing</i>	Means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms ‘Process’ and ‘Processed’ should be construed accordingly.
<i>Data/Record Retention Schedule</i>	The maximum period of time information/data should be retained by the LYIT for legal and business purposes. It is the responsibility of data owners to define the retention period for their records/data and the eventual fate of the records/data on completion of this period of time.

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.





lyit

Institiúid Teicneolaíochta

Leitir Ceanainn

**Letterkenny Institute
of Technology**

**Bóthar an Chalaigh, 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