Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Data Protection Procedures

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	
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

LYIT has adopted these Data Protection Procedures, which creates a common core set of values, principles and procedures intended to achieve a standard set of universal compliance parameters based on GDPR.

These procedures should not be viewed in isolation. Rather, they should be considered as part of the LYIT suite of Data Protection Policies (see Appendix A), in particular the Data Protection Policy.

These procedures have been agreed through a collaborative process at sectoral level. They are designed as sectoral templates offering guidelines to best practice in Data Protection. Each Institute will need to adopt and amend in accordance with local needs and requirements.

2. Data Protection Officer Information (DPO)

The Data Protection Officer (DPO) is available to provide support, assistance, advice and training to ensure that all relevant staff and students are in a position to comply with the legislation. The Institute encourages staff to raise questions about data protection matters and to report any issues or data breaches encountered at work.

3. Data Protection Privacy Notice Procedures

Schools and Departments must provide all of the following to Data Subjects in the form of a fair disclosure notice at Personal Data collection point of:

- Data Controller's name and business address.
- DPO's business address.
- Information Collection purpose.
- Information processing legal basis.
- Identities/Categories of all natural/legal persons to whom the Data controller could or may send Personal Data (Joint Data Controllers or other Data Processors).
- Whether LYIT will or could transfer Personal Data outside of the European Economic Area and if the EU Commission has not determined if the recipient jurisdiction/country has adequate Data Protection laws in place.
- The information transfer terms i.e. pursuant to a contract including EU Commission's Model Contractual Clauses, or other legally approved mechanism.
- Notice of the Data Subject's various GDPR rights including access rights, rectification, erasure, correction, restriction on processing, objection and portability of Personal Data held about them, and the means of exercising those rights (for example, who to contact).
- How long LYIT expects or intends retaining the Personal Data.
- Notice of the Data Subject's right to lodge a complaint with the supervisory authority and the Institute's lead supervisory authority details.
- Notice of statutory or contractual requirements require this Personal Data provision request.
- Notice of whether the data subject is obliged to provide the Personal Data and the consequences of not providing the Personal Data.
- If Processing involves automatic decision making or profiling than the notice should provide meaningful information about the automatic decision making logic and consequences of the Processing for the Data Subject.

- Any other information to guarantee "fair processing", as deemed necessary by the School or Function in consultation with the DPO. For example, LYIT should disclose where it may use the Personal Data in a manner not apparent to the Data Subject.

If the School and Departments intends to process Personal Data for an additional process outside of original consent then the School and Function must get the Data Subject's additional consent through an additional fair disclosure notice.

Wherever possible, these disclosures should be given at the first point of contact with the Data Subject or, if it is not possible on collection, as soon as reasonably practicable thereafter, unless otherwise agreed with the DPO in consultation with the Data Protection Oversight Committee. In the case of employees, the disclosures should be made in the employment contract. Appropriate disclosures should also be made in any job application form, employee handbook or other internal employment document. The disclosures should be made in a manner calculated to draw attention to them.

The fair disclosure notices content and mechanism requires prior DPO approval in consultation with the Head of School or Function.

Please refer to Appendix B for an example of a Privacy Notice Requirements Checklist.

4. Data Storage Limitations Procedures

School and Functions must only keep Personal Data for the period necessary for permitted uses as per the Data Retention Policy.

School and Functions should erase any Personal Data that violates:

- Data Protection Law
- Data Protection Regulations
- Contractual Obligations
- Requirements of the Data Protection suite of policies (Appendix A)
- If the Institute no longer requires the Data
- If the Personal Data no longer benefits the Data Subject in the relevant process.

School and Functions should Anonymise and / or Pseudonymise Personal Data (please refer to Data Encryption & Data Anonymisation and Pseudonymisation Policy) rather than erase if:

- The law prohibits erasure;
- Erasure would impair the legitimate interests of the Data Subject;
- Erasure is not possible without disproportionate effort due to the specific type of storage; or
- Where the Data Subject has disputed the accuracy of the Personal Data, the Institute disagrees with that assertion and resolution has not been reached.

5. Security of Personal Data Procedures

When implementing Personal Data security measures each School and Function must consider:

- Technological developments
- Implementation Costs
- Nature of relevant Personal Data
- Inherent Risks posed by human action/physical/natural environment

IT management must adequately relate EU Data Protection requirements to relevant LYIT IT Policies, Procedures and Programs.

6. Data Protection Impact Assessments

If the School and Function considers that particular Personal Data Processing may affect a Data Subjects rights and freedoms than they should:

- Engage the DPO in terms of the issue.
- Conduct a Data Protection Impact Assessment (DPIA).

Refer to Appendix D for a Data Protection Impact Assessment Examplar.

7. Data Processing Activity Inventory Procedures

Each School and Department must maintain a written record of processing activity under its responsibility.

When Operating as a Data Controller

When operating as a Data Controller, each School and Department must maintain a written record of processing activities to include:

- Data Controller name and contact details (and joint controller if applicable), the Data Controller's representative and the DPO
- The Processing purposes
- Data Subjects category description
- Personal Data category description
- Personal Data disclosure recipient categories
- If outside the European Economic Area, the recipient identification, country and Personal Data protection relevant transfer mechanisms and safeguards
- Personal Data erasure time limits by category
- Personal Data safeguarding technical and organisational security measures

When Operating as a Data Processor

When operating as a Data Processor, each School and Function must maintain a Processing activity written record when carried out on a Data Controllers behalf for the Processing relationship lifetime. That record must, at a minimum, retain the following information:

- Data Processor name and contact details and of each Data Controller which the Data Processor is acting on behalf of
- Data Processor's representative name and contact details, the Data Controller's representative, and the DPO
- The Processing categories carried out on behalf of each Data Controller
- If outside the European Economic Area, the recipient identification, country and Personal Data protection relevant transfer mechanisms and safeguards
- Personal Data safeguarding technical and organisational security measures

Data Processing Activity Inventory Maintenance

School and Departments must maintain all completed processing activity records on a system accessible to the DPO. The DPO will review these records periodically and will update same accordingly, in consultation with the Data Controller. The DPO will provide Processing Activity records to a supervisory authority on request.

Refer to Appendix C for a template for documenting the Data Processing Register.

8. Third Party Transfer Procedures

School and Departments must not transfer Personal Data to a Third Party outside of the EEA regardless of whether the Institute is acting as a Data Controller or Data Processor unless:

- The EU recognises the transfer country/territory as having an adequate level of Data Subject legal protection relating to Personal Data Processing or
- The EU recognises the transfer mechanism as providing adequate protection when made to countries/territories lacking adequate legal protection.
- The original Personal Data consent explicitly allows Third Party transfer or transfer is authorised by law.
- All reasonable, appropriate and necessary steps have been taken to maintain the required level of Personal Data Protection; and
- LYIT Solicitor has provided advice that necessary contractual provisions support the transfer.

Subject to the provisions above, including any necessary LYIT approvals, School and Functions may transfer Personal Data to a Third Party outside of the EEA where any of the following apply:

- The Data Subject has given explicit Consent to the proposed transfer; or
- The transfer is necessary for the performance of a contract between the Data Subject and LYIT, or the implementation of pre-contractual measures taken in response to a request by a Data Subject; or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between LYIT and a Third Party; or
- The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims; or
- The transfer is required by law; or
- The transfer is necessary to protect the Data Subject's vital interests; or
- The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

The DPO and LYIT's Solicitors must assess whether any of the above exceptions apply prior to any Personal Data transfer and must record the determination in writing.

9. Thirds Party Relationships Procedures

Where a School and Function engages a Third Party for Processing activities, this Data Processor must protect Personal Data through sufficient technical and organisational security measures and take all reasonable compliance steps.

When engaging a Third Party for Personal Data processing, School and Functions must enter into a written contract, or equivalent. This contract or equivalent:

- Shall clearly set out respective parties responsibilities
- Must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.

School and Functions must ensure that all Third Party relationships are established and maintained.

10. Subject Access Request (SAR) Procedures

Employees and students of LYIT should contact the Data Protection Officer to discuss their request requirements prior to making a formal request in order to maximise the likelihood that their request will be fulfilled in a timely, efficient and satisfactory manner. External requests for personal data should all be directed to the Data Protection Officer for response.

All subject access requests must be made via the Subject Access Request (SAR) form (see Appendix E.) that is available on the Institute website. All subject access requests shall be directed to the Data Protection Officer and all requests shall have an open status until an action by the Data Protection Officer sets a closed status.

The Data Protection Officer upon receipt of the request shall in the following order:

1. Contact the data subject or their representatives confirming receipt of the request along with the date the request was received. In addition, if there is any doubt regarding the identity of the requestor, the Data Protection Officer may request a valid photo ID as additional proof of identity.
2. Determine if the request should be refused under GDPR. If the request is to be refused then the Data Protection Officer shall contact the data subject to inform them of this and shall set the status of the request as closed providing details of the case closure.
3. Determine the effort involved in satisfying the request. If the Data Protection Officer determines that the effort involved means:
    a) The request cannot be satisfied within the 1 month GDPR timeline but can be satisfied with an extension then the Data Protection Officer shall contact the requester and inform them of the need for an extension as well as the reason why an extension is required, and also an approximation of when the request requirements will be met. This contact shall be documented on the open request.
    b) There is a requirement for the charging of a fee then the Data Protection Officer shall contact the requester and inform them of this need. The requester must then decide whether they are proceeding with the request or whether they wish to terminate the request. This contact shall be documented on the open request and depending on the decision of the requester shall either close the request or continue to fulfil the request.
4. The Data Protection Officer shall proceed to fulfilling the request. Once the request is completed then the Data Protection Officer shall contact the requester telling them that the request is available in the format

that they requested and that they should call for collection, or if it is an external requestor, that the request will be sent via official correspondence once their identity has been confirmed (see next step).

5. The Data Protection Officer shall verify the identity of the requester by their employee ID card/student ID card (if internal requestor) or official ID documentation (e.g. passport, driver's license) (if external requestor) before the transfer of data is complete.
6. The Data Protection Officer shall close the open request.

Refer to Appendix E for further guidance on addressing Subject Access requests

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
- 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: PRIVACY NOTICES REQUIREMENTS

Have you reviewed your privacy notices yet? Do they include the following?

Identity and contact details of the controller	☐
Contact details of the Data Protection Officer	☐
Details of the purposes and legal basis for the processing of personal information	☐
Details of the legitimate interests the processing is based on (if applicable)	☐
Recipients of the personal data	☐
Details of transfers to third countries and the safeguards that are in place (if applicable)	☐
Details of how the data subject can obtain a copy of data transferred to third countries and how to obtain a copy of this data	☐
Retention period or the criteria used to determine a retention period	☐
Details of the data subject's right of access to and deletion/rectification of personal data, their right to objection to processing &portability	☐
Details of the right to withdraw consent (if applicable)	☐
The data subject's right to lodge a complaint with the supervisory authority	☐
Details of the consequences when a data subject neglects to provide personal data when they are obliged to do so	☐
Details of automated decision making (if applicable) including logic used and consequences to the data subject	☐

APPENDIX C: DATA PROCESSING REGISTER EXAMPLE

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 t be GDPR compliar / methods of destruction
1																
2																
3																

APPENDIX D: DATA PROTECTION IMPACT ASSEMENT EXAMPLAR

PROCEDURES

Background

Data Protection Impact Assessments ('DPIAs') can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect LYIT. DPIAs are mandatory for any new high risk processing projects.

When to use a DPIA

Under the GDPR, a DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons." This is particularly relevant when a new data processing technology is being introduced. In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still good practice and a useful tool to help data controllers comply with data protection law. The DPIA should be carried out prior to the processing of data by LYIT.

Who must carry out the DPIA

It is the responsibility of the project team to ensure that a DPIA is carried out for any new high risk processing projects.

DPIA Process:

1. *Identifying whether a DPIA is required:*
   Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified

2. *Describe the information flows:*
   Describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

3. *Identify data protection and related risks*
   Identify the key privacy risks and the associated compliance and corporate risks.

4. *Identifying data protection solutions to reduce or eliminate the risks*
   Describe the actions you could take to reduce the risks, and any future steps which would be necessary.

5. *Signing off on the outcomes of the DPIA*
   Ensure appropriate sign off of outcomes is formally documented and retained.

6. *Integrating data protection solutions into the project*
   Ensure the controls and actions identified are tracked through to completion to ensure the rights of the data subject are upheld.

Template

1. Identifying whether a DPIA is required Please answer the screening questions below	
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used or in a way it is not currently used?	
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	
Will the project require you to contact individuals in ways that they may find intrusive?	
Is a Data Protection Impact Assessment required to be performed? (If answering 'yes' to any of the above performing a DPIA is advisable)	

2. Describe the information flows	
Date of Assessment:	
Assessment performed by:	
Function/Department:	
Process Name:	
Description of the envisaged processing operations: (Including collection, deletion and use)	
Purposes of the processing:	
Legal basis for processing:	
Necessity of the processing (Justification)	
Proportionality of the processing (Estimated number of Data Subjects Affected)	
Individuals consulted during the performance of DPIA (Include internal and external consultations held)	

3. Identify data protection and related risks			**4. Identifying data protection solutions to reduce or eliminate the risks**				
No.	*Privacy Issue*	*Risk*	*Existing Controls Identified*	*Risk Rating L x I*	*Additional Controls/ Actions Required*	*Action Owner*	*Deadline Date*
1							

5. Signing off on the outcomes of the DPIA	
DPIA Assessment result: (Pass- risk eliminated, avoided or accepted; Fail- risk avoided)	
Approved by:	

6. Integrating data protection solutions into the project	
Next steps/Actions	

Guidance

Example Risks to Individuals:

- Inappropriate disclosure of personal data internally within the organisation due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by "hackers".
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Corporate Risks:

- Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
- Data breaches or failure to live up to customer expectations regarding privacy and personal data are likely to cause reputational risk.
- Public distrust of organisation's use of personal information may lead to a reluctance on the part of individuals to deal with the organisation.
- Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
- Failure to manage how your company keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.
- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against the organisation. Under the GDPR the organisation may also be liable for non-material damage.

Compliance Risks:

The organisation may face risks of prosecution, significant financial penalties, or reputational damage if it fails to comply with the GDPR. Individuals affected by a breach of the GDPR can seek compensation for both material and non-material damage.

Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Examples of data protection solutions:

- Deciding not to collect or store particular types of information.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.
- Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol.
- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.
- Assessing the need for new IT systems to safely process and store the data, and providing staff with training in any new system adopted.
- Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.
- Ensuring that individuals are fully informed about how their information will be used.
- Providing a contact point for individuals to raise any concerns they may have with the organisation.
- If using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

Risk Assessment Guidance

Likelihood/Potential for an Incident to occur	*Impact/Outcome of Incident*	*Risk Level Calculation L X I*	*Guideline Action Timetable*
1 - Rare No history of event occurring over period of years. This event may occur but in exceptional circumstances.	1. Minor compromise of privacy (e.g. un-sensitive personal data such as helpdesk ticket compromised)	1 – 2 Acceptable	No Action
2 - Unlikely The event would be expected to occur annually.	2. Minor data breach (e.g. inappropriate contact of data subject via email)	3 – 5 Low	Prioritise after medium risk actions complete
3 - Possible This could occur monthly, as such it has a reasonable chance of occurring.	3. Moderate data breach (Sensitive data e.g. payroll compromised)	6 – 10 Medium	Prioritise after high risk actions complete
4 - Likely Expected to occur at least weekly, the event will occur in most situations.	4. Significant data breach (Financial loss, severe stress for a data subject or data subjects	11 – 15 High	Prioritise Action as soon as Practical
5 – Certain Expected to occur almost daily, it is more likely to occur than not.	5. Major data breach (Risk of severe financial loss to a large number of data subjects)	16 – 25 Very High	Action Urgent

APPENDIX E

Data Protection
Subject Access Request

Details of Requester

Name: _____

Email address: _____

Telephone Number: _____

Student ID Number: (if applicable) _____

If you are a current or former staff member, please provide details of the Department:

_____

If neither a student nor staff member, please provide details of your relationship with the Institute:

_____

Form of Access

My preferred form of access is: _____

Details of Request

In accordance with data protection legislation, I request access to the following personal data that I believe LYIT holds about me:

☐ A description of the personal data held
☐ A copy of the personal data held

Please provide as much information as possible to help the Institute locate the information such as the time periods concerned, names of members of staff who you may have dealt with or who may be able to locate the information, the department or areas of the Institute that are most likely to hold the relevant information.

_____

_____

_____

I acknowledge that, before I am given access to personal information about myself, I may be asked for ID

Signed: _____ **Date:** _____

In most cases we will respond to your request within 30 days. If your request is particularly complex, we may have to extend this time by a further 60 days but we will inform you if this is the case and explain the reasons for the delay.

Office Use Only			
Date Received:		*Identify Verified:*	
Office Ref:		*Information Released:*	

APPENDIX F: GLOSSARY OF TERMS

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Records	ISO 15489 defines records as "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.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Metadata	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: • Title and description • Tags and categories • Who created and when • Who last modified and when • Who can access or update.
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.
Sensitive Personal Data	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.
Data	Data as used in these Procedures 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 these Procedures 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 LYIT has an ongoing relationship. Third Party relationships, for the purposes of these Procedures, 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 these Procedures, and any documents issued in support of these Procedures, not referenced in this Glossary of Terms section, shall have the same meaning as the GDPR and/or local requirements.

Data Protection Commissioner	Means the office of the Data Protection Commissioner (DPC) in Ireland.
Data Subject	Refers to the individual to whom Personal Data held relates, including: employees, students, customers, suppliers.
EEA	*European Economic Area* Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.
GDPR	Means EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data.
Processing	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.
Anonymised	Means the process of making Personal Data Anonymous Data. 'Anonymise' should be construed accordingly.
Pseudonymisation	Means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

All other terms used in these Procedures and any documents issued in support of these Procedures, 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 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