Privacy & GDPR

Policy & Procedure

DATE APPROVED	**22nd September 2021**
POLICY PREFIX	**ED**
POLICY NUMBER	**5**
VERSION NO	**V1**
REVIEW DATE	**July 2023**

Approved By: Academic/Governance QA Committee **Date:** 18/08/2020

Approved By: Tony O' Brien CEO **Date:** 22/09/2021

This policy pertains to **Northridge House Education and Research Centre at St Luke's Cork**, hereafter referred to as **the Centre.**

1. Purpose of Policy

This policy will explain the ways the Centre gathers, uses, discloses, and manages a customer or client's data. It will inform the Learner, Staff or any other entity that shares personal data with the Centre of how that data will be collected, stored, and used. The policy will enable the Centre to adhere to Data Protection Regulations.

2. Definitions

GDPR – General Data Protection Regulations

Data: means automated and manual data.

Data controller: means a body that controls the contents and use of personal data.

Data Processor: means a person who processes personal data on behalf of a data controller.

Data Subject: means an individual who is the subject of personal data.

Data Protection Officer: means the person designated by the organisation as having ultimate responsibility for data protection within the organisation including the duty to report any data breach to the Data protection commissioner.

Processing: means performing any operation or set of operations on the information or data including:

3. Scope of Policy

This policy applies to all employees, learners, contractors, stakeholders, and suppliers of the Centre whose data is stored on the systems in either hardcopy or softcopy formats.

4. Policy Statement

This statement sets out what the Centre does with ordinary personal information that is provided to the Centre and why such information is gathered. This document is being provided to learners in line with the Centre's obligations under the General Data Protection Regulations (GDPR) which came into effect on May 25th, 2018.

From this date learners will have several enhanced rights in relation to how the Centre manages their information including:

• Access and obtain a copy of personal data on request

• Request the organisation to change incorrect or incomplete data

• Object to a particular use of personal data for the Centre's legitimate business interests or direct marketing purposes

• In certain circumstances to have personal information deleted or the Centre use of personal data restricted

• A right to data portability

• To withdraw consent at any time where processing is based on consent

• Any questions regarding this statement and the Centre's privacy practices should be sent to the GDPR officer at the Centre in the first instance

• Learners have the right to lodge a complaint to the Data Commissioner's Office if they believe that the Centre has not complied with the requirements of the GDPR

5. Roles and Responsibilities

The Centre as Data Controller must adhere to the eight rules of Data Protection. The eight rules, which apply whether the information is held on a computer or in manual form are:

- Obtain and process information fairly.
- Keep personal data only for one or more specified, explicit, and lawful purposes.
- Process personal data only in ways compatible with the purposes for which it was given initially.
- Keep personal data safe and secure.
- Keep personal data accurate, and up to date.
- Ensure that personal data is adequate, relevant, and not excessive.
- Retain it for no longer than necessary for the specified purpose or purposes.
- Give a copy of his/her personal data to that individual on request.

Data Protection

Information Collection and Use

The Centre maintains a range of information management systems to support its operation, assist in decision making across the organisation plus support effective communication and sharing information with learners and other stakeholders.

The main data management platforms used by the Centre include:

Microsoft Office 365 – email, word processing and spreadsheets are used to support day to day office work, mobile working, and collation of student's details.

These systems collect and process data making it available to authorized personnel.

The Centre use a managed services provider to support its IT operations.

The Centre maintain access to QQI's QBS system through a password-protected link via www.qqi.ie . This is used by the administrator to upload learner data in support of learner certification and access other QQI systems e.g., validation services and Q-help. The course administrator inputs certification data to QBS which is verified by the Director of Education following verification form which is then signed off by both parties.

The personal information that the Centre collects from Learners might include name, address, e-mail address and contact telephone number, PPS number, date of birth, certification results.

The Centre may collect this information in a variety of ways including application forms, curriculum vitae's, identity documents, evaluation forms, or other forms of assessment.

The personal information the Centre holds and processes on learner's behalf will be used to enable the Centre to operate its business and manage its relationship with learners effectively, lawfully, and appropriately. This includes using information to enable the Centre to comply with relevant regulations and with legal requirements which allows the Centre to pursue its legitimate company interests and to protect its legal position in the event of legal proceedings. If Learners do not provide this data, the Centre may be unable in some circumstances to comply with its obligations.

The Centre may sometimes need to process Learner's data to pursue its legitimate business interests, for example to prevent fraud, administrative purposes or reporting potential crimes. The Centre will never process Learner's data where these interests are overridden by learner's own interests.

The Centre does not sell or rent learner's information to any third-party organisation for marketing, fundraising, or campaigning purposes.

When Learners give the Centre personal information it takes steps to ensure that this information is secure. Once the Centre receives information, it uses technical and organisational precautions to prevent the loss, misuse, or alteration of personal data.

Who will have access to the data?

Learner's information may be shared internally with staff for the purposes of normal business operations. The Centre will not share data with third parties without learner's permission or transfer it outside of the European Union.

How long will the Centre keep Personal Information?

The Centre will retain data for periods necessary to comply with legal obligations and for the duration needed to manage relationships with Learners and employees.

The Centre is committed to protecting and respecting each learner's privacy and will ensure that the following core principles of the GDPR are adhered to 1. Lawfulness, fairness, transparency; 2. Purpose limitation; 3. Data minimisation; 4. Accuracy; 5. Storage limitation; 6. Integrity & Confidentiality; 7. Accountability.

Ensure that data subjects are informed in advance of all possible and specific uses of their information.

Ensure they are informed of an optout option at any time and that if opted in there is a clear option to opt out.

Data Storage & Retention:

Minimising data storage, so that unwarranted storage is deleted within the following parameters.

Data Retention Periods (learner/HR/QA Data:

Types of personal data	**Retention Period**
Student Results	Indefinite
Financial Records	7 years -to comply with revenue and SLH
Student Assessments & Feedback	After ratification of results by relevant examination board, expiry of appeals and issuing of certificates.
Other data: communication & information stored relating to data subjects i.e., emails, letters etc	6 months unless there is a legal requirement to keep for longer pertaining to (for example) student assessment malpractice
Student Email Accounts	6 months after graduation unless learner has subscribed to mailing list
External Authenticator and Director of Education Reports etc	5 years

Keeping all stored data safe and secure with appropriate backup arrangements. Personal data is stored in locked filing cabinets only accessible by authorised personnel. Computers are password protected with each staff member with their own logins. Using all data only for the purposes which are agreed by the informed consent of the data subject. Written consent also stored securely.

Data Destruction

Once data in hard copy format has met their required retention period it is then transferred to archives or destroyed. Confidential files are destroyed by an external shredding company. Electronic files are deleted from all systems on which data is stored. Any other media is also destroyed in a confidential manner.

Procedures to access personal data held by the Centre.

Formal written application is made to the Director of Education via email who will respond within 14 days from receipt of the request.

6. Associated Documentation

Irish Legislation

General Data Protection Regulations (2018)

The Data Protection Act 1988 (The Principle Act)

The Data Protection (Amendment) Act 2003

7. Referenced Policies

St. Luke's Charity & Home Policy on Data Access Requests & SOP for Data Breaches

8. Monitoring and Review

Reviewed 3 yearly or more frequently as needed.