GENERAL DATA PROTECTION REGULATION (GDPR) POLICY
OPEN TRAINING COLLEGE

1. Introduction

The EU General Data Protection Regulation (GDPR), effective May 2018 confers rights on individuals as well as responsibilities on organisations processing personal data. Personal data, both automated and manual are data relating to a living individual who is or can be identified, either from the data or from the data in conjunction with other information.

2. Purpose

To outline how the OTC complies with its legal obligations in respect of data protection.

3. Scope

This policy applies to all students, prospective students, staff, stakeholders and suppliers of the Open Training College (OTC) whose data is stored on College systems or in handwritten or hard-copy filed formats.

There are 6 legal bases on which data may be processed:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

In relation to sharing student data for certification purposes, such as with Quality and Qualifications Ireland (QQI), the College will rely on the basis of the contract which has been undertaken with the student, so that this contract may be completed. For an instance such as Protection of Enrolled Learners (PEL), if this were invoked, College would rely on 'legal obligation'.

4. Policy Statement

OTC has existing arrangements in place with respect to data protection, under the Data Protection Acts of 1988 and 2003. These arrangements are hereby supplemented with regard to the Data Protection Act, 2018 and the General Data Protection Regulation (GDPR- Regulation (EU) 2016/679).

OTC 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 and confidentiality; 7. Accountability.

Specifically, OTC will strengthen its response to data protection responsibilities by:

(1) Revising all forms and methods of data collection to ensure that data subjects are informed in advance of all possible and specific uses of information, so that the subject is aware of the limited, and necessary cases where their data will be shared; such as with QQI for certification purposes.

(2) In the case of specific permissions (where the basis for data processing is not covered by contract completion or legal obligation): Ensuring that data subjects are informed of an opt-out option at any time, having opted in, and that a clear route to activation of this option is provided to all subjects.

(3) Minimising data storage, so that unwarranted storage is deleted, within the following parameters:

Area	**Maximum Storage Time**
Student Results	Indefinite – the College is required to retain data relating to student results, so that such information is available to students at any given future date, in order that they may verify their results, particularly in relation to progressing to other programmes.

Financial Records	7 years – to comply with Revenue and SMH (St. Michael's House) policies.
Student Assessments and Feedback	5 weeks from ratification of results by the relevant Examination Board. This allows for the appeal window to have closed.
Other data: Communication with and information stored relating to any of the data subjects outlined in (3.) Scope, above. For example, emails, written notes and letters to/from the data subject.	According to the current OTC GDPR Action Plan and in any case, no more than 7 years.
Student e-mail accounts	6 months after graduation.

(4) Keeping all stored data safe and secure, with appropriate back-up arrangements.

(5) In the case of specific permissions (where the basis for data processing is not covered by contract completion or legal obligation): Using all data only for the purposes which are agreed by the informed consent of the data subject. Written consent to such usage is also to be stored securely and in the case of students seeking QQI awards, specific consent will be stored on the pro forma consent forms supplied.

(6) Adding additional security for "Special Categories of Data". These will be stored with additional password protection, with access only to nominated staff members, such as the Programme Director or relevant Programme Administrator.

(7) Complying with any and all Subjects Access Requests (SARs) within the statutory timeframe allowed.

(8) Notifying the designated organisational Data Protection Officer (DPO) and Data Protection Commissioner of any personal data security breaches within 72 hours of such a breach occurring.

5. Roles and Responsibilities

The College Director has ultimate executive responsibility for the effective development and implementation of academic policies. The Head of Quality & Academic Affairs has overall delegated responsibility for coordinating the day to day operation of the policies and the development, maintenance and monitoring of supporting procedures. All staff members are responsible for

pursuing the implementation of these policies in relation to data storage activities with which they are involved as part of their daily duties.

Further specific responsibilities are outlined in the Procedures attached to this policy.

6. Definitions

Data means automated and manual data. Automated data means any information on computer, or information recorded with the intention that it be processed by computer. Manual data means information that is recorded as part of a relevant filing system or with the intention that the data form part of a system.

Data Controller means a body that, either alone or with others, controls the contents and use of personal data.

Data Processor means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the programme of his employment.

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

Data Protection Officer (DPO) means the individual who is identified and 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.

Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Processing means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

- Obtaining, recording or keeping the information, or
- Collecting, recording organising, storing, altering or adapting the information or data,
- Retrieving, consulting or using the information or data
- Disclosing the information or data by transmitting, disseminating or otherwise making them available, or
- Aligning, combining, blocking, erasing or destroying the information or data.

Relevant Filing System means any set of information relating to individuals to the extent that, while not computerised, is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Special Categories of Data (*formerly* ***Sensitive Personal Data)*** means personal data which relate to specific categories defined as:

- The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject
- Trade union membership
- The physical or mental health or sexual life of the data subject
- The commission or alleged commission of any offence by the data subject or
- Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Subject Access Request (SAR) means a request, made by an identified data subject, for provision of data held by an organisation on that data subject. All data requested must be supplied to the data subject within 30 calendar days and there cannot be a charge for fulfilling this obligation on the first such request from a data subject. Second and subsequent requests may attract a charge.

7. Related Documentation

This policy should be read in conjunction with *GDPR policy Procedures.*

8. Contacts

The Head of Quality & Academic Affairs/Corporate Services Manager.

Policy Title:		**General Data Protection Regulation (GDPR)**
OTC Policy No		**1808**
Version		**1.2**
Date approved: March 2019	**Date policy will take effect:** April 2019	**Date of Next Review:** Annual
Approving Authority:		Academic Council
Document Owner/Contact:		Head of Quality & Academic Affairs Corporate Services Manager
Supporting documents, procedures & forms of this policy:		▪ Procedure for Data Protection: Open Training College ▪ GDPR Audit ▪ OTC GDPR Action Plan
Audience:		Public – accessible to anyone
Reference(s)		▪ EU General Data Protection Regulation, 2018 ▪ (Regulation (EU) 2016/679) ▪ Data Protection Act, 1988 ▪ Data Protection (Amendment) Act, 2003 ▪ Data Protection Act, 2018