# 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.

**Data Protection Practice / Accountability Requirements**

*Data Protection by Design and by Default:*

**Privacy by Design** is an essential requirement that involves minimising privacy risks to individuals. It is the consideration of data protection implications at the start or re-design of any product, service, system, IT application or process that involves the processing or personal data. It fosters a culture of embedding privacy by design into operations and ensuring proactivity instead of reactivity.

**Privacy by Default** promotes that, where possible, having regard to business implications and the rights of the data subject, the strictest data protection settings are applied automatically to any project.

The College has an obligation under GDPR to consider Data Privacy throughout all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to Personal Data. This is of particular importance when considering new processing activities or setting up new procedures or systems that involve Personal Data. GDPR imposes a 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought. The College when engaged in projects, new courses, services or systems development of any sort (including change to existing practices) through the relevant local project and change management processes must comply with the terms of this Policy and any specific guidelines and requirements set by the Data Protection Officer or ICT Policies in furtherance of these principles.

**Data Protection Impact Assessment (DPIA)**

When the College undertakes a processing activity which would be likely to have a privacy impact upon students or staff, they should consider if a Data Protection Impact Assessment is required. A Data Protection Impact Assessment (DPIA) is a tool, required by GDPR, which can help the College to identify the most effective way to comply with its Data Protection obligations as well as meeting individuals' expectation of privacy by facilitating the identification and remediation of risks in the early stages of a project. It should also identify measures which would help to reduce risks. Therefore, DPIA's are an integral part of taking a Privacy by Design approach to processing of Personal Data.

When the Processing of Personal Data may result in a high risk to the rights and freedoms of a Data Subject, the College is required to conduct a DPIA and then consult with the Data Protection Officer. Where the requirement for a DPIA has not been established, or where there is any confusion as to the applicability of Data Protection requirements, a referral must be made to the DPO and the Privacy by Design principles.

**Record of Processing Activity and Data Inventories**

The College as a Data Controller is required under GDPR to maintain a record of processing activities (ROPA) under its responsibility. That record contains details of why the Personal Data is being

processed, the types of individuals about which information is held, who the Personal Data is shared with and when such Data is transferred to countries outside the EU.

New activities involving the use of Personal Data that is not covered by one of the existing records of processing activities require consultation with the Data Protection Officer prior to the commencement of the activity.

**Data Inventories**

The College has created a Data Inventory / Data Processing Register Template as part of the GDPR compliance program. This details all business activities that involve the processing of personal data, the basis for doing so, retention periods for this personal data, what the personal data is used for, and whether this personal data is transferred to a third party.

Maintenance of Data Processing Inventories:

The College must maintain a written records of processing activity under its responsibility on a system accessible to the Data Protection Officer. The Data Protection Officer can review these records periodically and will update same accordingly. The Data Protection Officer will provide Processing Activity records to a Supervisory Authority (Office of the Data Protection Commissioner) on request.

**Transfer and Sharing of Data**

Sharing with a Third Party or External Processor

As a general rule, Personal Data should not be shared with or passed on to third parties, particularly if it involves Special Categories of Personal Data but there are certain circumstances when it is permissible e.g.

- The College may disclose student's Personal Data and Sensitive Personal Data (Special Category Personal Data) to external agencies to which it has obligations or a legitimate reason. Examples are listed in Appendix 1.
- The Data Subject consents to the sharing.
- The third party is operating as a Data Processor and meets the requirements of GDPR. Where a third party is engaged for processing activities there must be a written contract or equivalent in place which shall clearly set out respective parties responsibilities and must ensure compliance with relevant European and local Member State Data Protection

requirements/legislation. The Data Protection Officer should be consulted where a new contract that involves the sharing or processing of personal data is being considered.

Transfer of Personal Data outside the EEA

Transfers of Personal Data to third countries are prohibited without certain safeguards. The means the College must not transfer Personal Data to a third country unless there are adequate safeguards in place which will protect the rights and freedoms of the Data Subject. It is important to note that this covers Personal Data stored in the cloud as infrastructure may be in part located outside of the EU/EEA.

The College must not transfer Personal Data to a third party outside of the EU/EEA regardless of whether the College is acting as a Data Controller or Data Processor unless certain conditions are met.

Prior to any Personal Data transfer outside the EU/EEA, the Chief Operations Officer, (on the recommendation of the Data Protection Officer) must approve the transfer of such information and the Data Protection Officer will record the determination in writing.

**Third Parties Relationships and Data Sharing Agreements**

Where the College engage a third party for processing activities, the 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 Functional Areas must enter into a written contract, or equivalent. This contract known as a Data Sharing Agreement and must:

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

and must give due consideration to the following items:

- Management of Data Processors
- Selection of Data Processors
- Contract Requirements
- Sub-contracted Data Processors
- Monitoring and Reporting

- Data Transfers
- Appropriate Safeguards
- Derogations for specific situations
- Once off transfer of Personal Data
- Data Sharing Agreements
- Review of data sharing arrangements
- Data transfer methods
- Email
- Cloud storage and cloud applications
- Telephone / mobile phone
- Sending the information by post
- Hand delivery / collection
- Data Breach Notification

**Data Subjects' Rights**

Data Subjects have the following rights under Data Protection Law, subject to certain exemptions, in relation to their personal data:

| Right | Explanation |
|---|---|
| Information | The right to be informed about the data processing the University does. |
| Access | The right to receive a copy of and/or access the personal data that the University holds about you. |
| Portability | You have the right to request that the University provides some elements of your personal data in a commonly used machine readable format in order to provide it to other organisations. |

| Right | Explanation |
|---|---|
| Erasure | The right to erasure of personal data where there is no legitimate reason for the University to continue to process your personal data. |
| Rectification | The right to request that any inaccurate or incomplete data that is held about you is corrected. |
| Object to processing | You can object to the processing of your personal data by the University in certain circumstances including direct marketing material. |
| Restriction of processing concerning the data subject | You can request the restriction of processing of personal data in specific situations where:<br>i. You contest the accuracy of the personal data<br>ii. You oppose the erasure of the personal data and request restriction instead<br>iii. Where the University no longer needs the data but are required by you for the establishment, exercise or defence of legal claims |
| Withdraw Consent | If you have provided consent for the processing of any of your data, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn. This can be done by contacting the department who obtained that consent or the University's Data Protection Office (contact details below). |
| The right to complain to the Data Protection Commissioner | You have the right to make a complaint in respect of our compliance with Data<br><br>Protection Law to the Office of the Data Protection Commissioner. |

In order to exercise any of the above rights, please contact a representative of the Data Protection Officer using the contact details in Section 8 below.

## 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.

***Appendix 1***

Below are some examples of when the OTC will release data about you to third parties (i.e. outside the OTC) where we have a legitimate reason in connection with your studies or with your explicit consent.

The OTC may share your relevant personal data with bodies including the following:

- Data Processors (sub-contractors used by OTC in order to carry out a function for the University) e.g. Wholeschool, MIT Education Solutions
- Software providers or service providers performing administrative functions on behalf of OTC (e.g. SMH IT services)
- Quality and Qualifications Ireland (QQI)
- Department of Social Protection to verify employment status and eligibility for allowances
- Revenue Commissioners
- Other funding bodies
- Professional and regulatory bodies where programmes are accredited by such bodies
- Work placement / Internship providers
- Research funding bodies
- Other higher education institutions, partners or research organisations to which a student transfers or pursues an exchange programme or where a student's programme is being run collaboratively
- External examiners
- Direct mail agencies/printing companies to facilitate the delivery of mailshots Sponsors funding student prizes and awards
- Plagiarism detection service providers to ensure academic standards
- Learning Support Service Providers
- Potential employers/recruitment companies for verification of qualifications
- Irish Survey of Student Engagement (ISSE)
- Photographers, videographers and media personnel to facilitate the marketing, promotion and documentation of activities in the College
- Irish Naturalisation and Immigration Service
- Insurance companies for Accident/Incident Report Forms for accidents occurring within the College. Insurance companies for claims made under Student Personal Accident Policy College legal advisor
- An Garda Síochána to assist in the prevention or detection of crime
- Auditors
- Realex (Payment Service Provider)
- Other HEIs for Student Fee Declaration Form
- Redaction service providers

This is not an exhaustive list and any other disclosures to third parties not listed here are made only where there is legitimate reason to do so and in accordance with the law.

| | | |
|---|---|---|
| **Policy Title:** | | **General Data Protection Regulation (GDPR)** |
| **OTC Policy No** | | **1808** |
| **Version** | | **1.3** |
| **Date approved:**<br>June<br>2021 | **Date policy will take effect:**<br>June 2021 | **Date of Next Review:**<br>Annual |
| **Approving Authority:** | | Academic Council |
| **Document Owner/Contact:** | | Head of Quality & Academic Affairs<br>Corporate Services Manager |
| **Supporting documents, procedures & forms of this policy:** | | ▪ Procedure for Data Protection: Open Training College<br>▪ GDPR Audit<br>▪ OTC GDPR Action Plan |
| **Audience:** | | Public – accessible to anyone |
| **Reference(s)** | | ▪ EU General Data Protection Regulation, 2018<br>▪ (Regulation (EU) 2016/679)<br>▪ Data Protection Act, 1988<br>▪ Data Protection (Amendment) Act, 2003<br>▪ Data Protection Act, 2018 |