SECTION 8: INFORMATION AND DATA MANAGEMENT

Supporting Documents:

1. Freedom of Information Acts 1997, 2003 and 2014

2. Data Protection Acts of 1988, 2003 and 2018.

3. General Data Protection Regulation (GDPR- Regulation (EU) 2016/679)

8.1 Information Systems

8.1.1 IMS

The key system for information collection and storage within the College is the Information Management System (IMS), which has been specifically designed and tailored to meet the needs of the College. Each new student registered with the College is assigned a unique student number on the system, which remains with them for the duration of their studies with the College. Access to the system is strictly limited to internal College staff, with varying levels of access for teaching and administration staff. Amendments to information held on the system may only be made by authorised personnel of the Administration Department following receipt of written confirmation of the required changes.

8.1.2 Survey Monkey

All staff, student, graduate and other stakeholder surveys are administered using Survey Monkey online surveying tools (www.surveymonkey.com). This system allows for the easy dissemination of surveys through e-mail or online channels. Data gathered is stored online in a private account, accessible only by authorised College staff. The system also facilitates basic analysis of the data or exporting of the data to other computer applications for more advanced analysis. Participation in these surveys is on a voluntary basis and the identities of respondents are protected in all publications of survey results.

8.1.3 Assessment Broadsheets

Broadsheets of assessment results are completed for each academic year and uploaded to QQI's QBS for certification of students' academic achievements. These electronic broadsheet files are stored indefinitely in the secure filing system of the college, accessible only to internal College staff and may only be amended by authorised personnel of the Administration Department. Any

amendments required to broadsheets following their ratification by Examination Board will be notified, in writing by the Head of Quality & Academic Affairs, to the External Examiner(s) and QQI.

8.2 Learner Information Systems

8.2.1 Personal Data

Personal identifying information on all students is gathered and maintained for the purpose of providing an individually tailored service to each student, and for registering students for certification with accrediting bodies.

This information is collected for each individual student as part of the application process, and is updated each year through the re-registration process. All personal student information collected through these processes (i.e. name(s), addresses, email, contact telephone numbers, PPSN, gender, nationality, country of birth, occupational status.) is inputted into the College Information Management System (IMS), updated annually, and maintained indefinitely. A student will be facilitated to register a change in their personal details at any stage of their studies. To facilitate a name change students are required to submit suitable identification with the desired name (i.e. birth certificate/marriage certificate). This documentation will be forwarded to the relevant accrediting body and maintained on file by the College.

At the application/registration stage, students are also informed of the College's obligation to share this information with QQI/Other relevant bodies, in a case where the Protection of Enrolled Learners (PEL) arrangements are invoked. Students are informed of any changes within 14 days of such change.

Additional hardcopy documentation gathered in the application process is maintained for the period of registration of the individual student. This can include:

- Application form
- Photographs
- Copy of ID (driver's licence/ passport)
- Copy of visa (International students)
- Previous educational transcripts
- Volunteer declaration form
- Academic reference (Advanced Entry students)
- CV (Advanced Entry students)

- English proficiency evidence (International students)
- Interview record form

The tutorial support function generates significant records regarding individual students' progress with their studies. The College is committed to ensuring that sufficient data is gathered and stored to ensure the ongoing provision of a high standard of service and support to students, while respecting individual student needs for confidentiality.

The following records are maintained for the period of student registration on a programme to ensure continuity in the provision of tutorial supports, to facilitate any transition in tutors and to ensure consistency in the application of College policy and procedures:

- Individual student tutorial records;
- Assignment extension applications;
- Medical certificates;
- Records of all online activity of students, including assessment activities completed online.

Tutorial information which may be called upon after student graduation is maintained by the College indefinitely. This information may be relevant to students who progress to further education or who appeal assessment results to the accrediting bodies, for example. The following records are maintained indefinitely by the College:

- All formal written correspondence between tutors and students;
- All original documentation relating to additional supports or assessment accommodations implemented (e.g. for reasons of disability/medical condition/specific learning difficulty);
- Records of assessment appeals and outcomes;
- Records of disciplinary procedures and outcomes (including any plagiarism investigations).

8.2.2 Academic Performance and Achievement

Details of programmes, modules and assessments completed by students are recorded by the College and maintained indefinitely, to facilitate the certification of students' work through the accrediting bodies as well as facilitating access, transfer and progression for students.

All marks achieved by students in assessments are recorded and maintained in secure Excel files, on the College IMS and on the QBS, which are updated on completion of each module. Internal Broadsheets are produced and these are finalised and signed on conclusion of the Examination Board meeting. Following the meeting the agreed marks are signed off by the Academic Manager

on the QBS for issuing of certificates. Electronic copies of the broadsheets are maintained on computer file indefinitely, to facilitate the provision of transcripts and reprints of Diploma Supplements.

For each year of their studies with the College, each student is assigned a file, which is maintained by their Tutor and in which the following are stored:

- All work submitted by the student for assessment;
- Completed rubric for each assessment;
- Copy of written feedback given to student on assignments;
- Copies of appropriate documentation regarding assessment supports and/or accommodations implemented;
- Records of assessment appeals and outcomes.

In addition to this hardcopy record all assignments (excluding appendices) submitted through Turnitin.com are maintained indefinitely as electronic files, and rubrics, with feedback to students, are filed and maintained indefinitely on the College's secure IT system.

On conclusion of the Appeals Process timeframe, hardcopies of all ratified assessment scripts and related materials will be destroyed (using a certified document destruction contractor) within 4 weeks. Students are advised to keep a copy of all work, which they submit to the College for assessment, as this cannot be returned.

Where a student has delayed completion of their studies, the following system applies to the storage of students' work:

- Students' work that has been assessed and ratified by the Examination Board will be destroyed within 4 weeks of the meeting, as the corresponding credits will have been awarded to the student by this time.
- Assignments and examinations, which have been completed but not ratified by the Examination Board, will be considered invalid after a two-year period.
- The work of any student, who wishes to return to the Open Training College more than two years following their withdrawal, will be reviewed individually by the Programme Director, and the student may be required to attend a viva voce and/or resubmit work. This is to ensure that the student's knowledge and skills are sufficiently current and relevant for them to continue with their studies.

8.2.3 Student Feedback

Student satisfaction with and feedback on the programmes and services of the Open Training College is garnered through a series of module and end of year surveys administered online, with each individual student. In these surveys, students are invited to give their feedback on the module and programme content and delivery, the tutorial and other learning supports, and the subsidiary support services offered by the College.

This feedback is collected by e-mail invitation to each individual student. Responses to all surveys are treated as confidential and identifying information of respondents is not contained in any published material. However in the case of inappropriate use of the surveys individual responses may be altered or removed, as deemed appropriate by the College. The College also reserves the right to track responses to the individual user to be followed up as appropriate.

Inappropriate use of the surveys includes the identification of any staff member or student by using their name in a response, and the use of language that may be considered defamatory, obscene, threatening or offensive. Students are provided with appropriate usage guidelines before commencing any survey.

8.3 Management Information Systems

As is detailed in this document the College has a well-functioning quality assurance management system that produces ongoing evaluative information about results and processes. Management and College staff can then use this information to respond, develop policies and procedures and take actions that contribute to strategic/operational management and continuous improvement, which is at the core of our quality assurance system.

The management process assisted by the information generated by the QA system includes sequential planning and management activities such as strategic management and objectives, the planning of operations and resources, implementation and monitoring, and finally, the evaluation of results and process performance. The strategy process produces the strategic objectives for the planning period. The operations of the internal processes are aligned with budgeting and human resources planning. The achievement of results is regularly monitored and ensured to achieve the desired objectives during the planning year. Finally, the achievement of objectives is evaluated and reported to stakeholders.

8.4 Information for Further Planning

All of the data gathered by the College, as indicated throughout this Quality Assurance Document provides important information to the College about the success of its endeavours, areas requiring improvement and opportunities for further developments. All data which is considered to be a critical quality indicator is carefully considered by the Academic Council and/or the appropriate subcommittee of the Council, and forms the basis upon which recommendations are made to amend, develop and improve programmes and services. Data, which are considered to be critical quality indicators, include:

- Student registration and re-registration numbers
- Withdrawal numbers
- Programme and stage completion rates
- Assessment results
- Staff and student feedback
- Survey response rates
- Quality assurance recommendations and follow-up

8.5 Completion Rates

Completion rates are recorded in the first instance on the cover page for the External Examiner's report. The information given will show, in relation to the specific programme, the number of students who:

a. Started; b. Withdrew; c. Passed or failed; and d. Completed (and relative percentages).

Additional information will also be presented regarding the percentage of students achieving particular grades. This data will then be analysed in the annual QA report for programmes, in conjunction with Student end-of-year feedback and Programme Board improvement plans.

Completion statistics can then be used to allow benchmarking against other internal and external (sectoral, discipline area, national, international) cognate programmes.

8.6 Records Maintenance and Retention

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: i. You contest the accuracy of the personal data ii. You oppose the erasure of the personal data and request restriction instead 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 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: June 2021	**Date policy will take effect:** June 2021	**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

8.6.2 Procedure for Data Protection

Procedure Outline / Method(s) used to carry out this procedure	Responsibility of	Evidence generated by this procedure to ensure its effectiveness
1. Revision of forms/IMS terms and conditions	Head of Quality & Academic Affairs, Programme Administrator, Corporate Services Manager, Head of E-learning	Updated forms to be stored on the shared drive. Specific use of data to be outlined at point of data collection. Terms and conditions attached to student registration to be agreed by data subject at time of registration on the College's Information Management System (IMS).
2. Opt-out	As above.	In the case of specific permissions (where the basis for data processing is not covered by contract completion or legal obligation): Opt-out at time of data collection or any future stage to be specified on all above collection modes. Default opt-out point of contact is: enquiries@opentrainingcollege.com
3. Retention/Deletion	Programme Directors and Managers (College Executive Committee) executive committee. Teaching, Learning & Assessment Committee. Collaborative Partners. Corporate Services Manager, Head of Quality	Retention periods to be specified in GDPR Action Plan. Current periods to be published in Student Handbooks and on OTC and Collaborative Partner websites. Deletion schedule to be agreed by CSM and HQ&AA in conjunction with College Executive Committee; to

	& Academic Affairs, CIT Support St. Michael's House.	take place twice annually in January and July. Physical deletion, timing and amount by agreement with St. Michael's House CIT Services, for soft data. Hard copy data to be deleted under current arrangements for professional and confidential shredding service.
4. Storage and Security	Head of Quality & Academic Affairs, Programme Administrators, Corporate Services Manager, Head of E-learning	All soft data to be stored on shared drive and IMS. Movement of data on secured, password protected and encrypted memory sticks. Back-up per St. Michael's House IT systems procedures. Particular arrangements for "Special Categories" at (5.) below.
5. Special Categories of Data *Relevant:* **1. Medical certificates** **2. Additional support reports**	Programme Directors, Designated Programme Administrator	Programme Directors to store sensitive information on students in a separate, password protected folder on the shared drive. Information relevant to workshops/assignments to be shared with designated programme administrators only. Hard copies of sensitive information are stored in a code-protected room (or temporarily in locked filing cabinet).
6. Subject Access Requests	Designated Administrator	All information relating to data stored on the relevant subject to be

		sent in hard copy to the subject making the access request, within 30 calendar days of such a request. If subject requests soft copy provision this may be supplied, as an alternative but only if this request comes from the subject. Hard copies to be sent by registered mail.
7. Breaches	Data Protection Officer (DPO) – St. Michael's House	Any data breach discovered to be reported immediately to the designated SMH Data Protection Officer (DPO). The DPO must inform the Data Protection Commissioner of any such breaches within 72 hours.

PEL and GDPR: All students are informed in the Terms and Conditions accepted at the time of registration that in the unlikely event of PEL procedures being initiated, their details may be shared with QQI and any other Colleges/Bodies which may act to "finish out" relevant programmes, as follows:

- Registration details
- Programme work to date
- Results achieved to date
- Copies of Assessments; Assignments/Examinations
- Any records of extension applications, appeals, repeats, resubmissions or disciplinary action

8.7 Data Protection and Freedom of Information

Data Protection

In accordance with its function the Open Training College (OTC) is required to collect, use and keep personal data and information for a variety of purposes about its staff, students and other individuals who come in contact with the College. The purposes of processing data about staff, students and other individuals with whom OTC has dealings include the organisation and

administration of programmes, evaluation activities, consultancy/project work, the recruitment and payment of staff, compliance with statutory obligations and compliance with legal obligations to funding bodies and government, etc.

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Act 1988, the Data Protection (Amendment) Act 2003 and the Data Protection Act 2018 (the Data Protection Acts) confer rights on individuals as well as responsibilities on those persons 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 that is in, or is likely to come into, the possession of the Data Controller.

This safeguarding has now been strengthened by the introduction of the GDPR in May 2018 (policy at 8.6.1, above).

Freedom of Information

The OTC recognises its responsibility under the Freedom of Information Acts 1997, 2003 and 2014, and the right of students to gain access to information held on them by the College, and will comply with any reasonable requests made under the Acts.

8.8 Integration with Blended Learning and Online Learning Strategy

The most pertinent elements relating to Blended Learning (BL) and Online Learning (OL) in this section are:

- The Information Management System (IMS)
- Survey tools
- Policy and procedures for Data Protection & the General Data Protection Regulation (GDPR)
- Special categories of data
- Subject Access Requests (SARs)
- Assessment, feedback and rubrics
- Management Information Systems (MIS)

Blended Learning: This section meets **"***Topic Specific Statutory Quality Assurance Guidelines for Providers of Blended Learning Programmes*" (QQI, 2018), in relation to the following:

i. Tracking learner progress and achievement, marking and returning assessments, and providing feedback to learners and assessors are fit-for-purpose in an online learning context.

ii. Clarity in any additional registration arrangements deemed necessary by the provider.

iii. Policies, regulations and processes (including administration) are fit-for-purpose in the context of blended learning.

iv. Arrangements for assuring compliance with any legal or regulatory obligations are appropriate to the blended learning and online learning context.

v. Clear parameters on data protection including the General Data Protection Regulation (GDPR).

vi. Mandatory training includes child protection, intellectual property and copyright, and protection for enrolled learners.

vii. A planned approach to the procurement of services (e.g. cloud services), hardware and software to support online learning and a clear policy on a common platform for approval of exceptions.

viii. Contingency arrangements in the event of platform, hardware or software failures.

ix. A student record system designed or adapted to support blended learning programmes and learners and their quality assurance.

x. There are nominated academic/professional moderators who understand and have the authority to intervene in, for example, cyber bullying that may constitute risk to learners and/or the provider.

xi. Processes for learner records are sufficient and accurately maintained, and up-to-date learner records are available for monitoring progression and achievement.

xii. Privacy laws on data protection are appropriate for all aspects of online provision. Learner concerns about the confidentiality of learner records are respected.

xiii. A unique learner identity used by the provider; that protects learners and indicates their own electronic trail or digital persona.

xiv. Mechanisms that facilitate a safe, accessible and reliable blended learning environment for all learners. These mechanisms promote dignity, courtesy and respect in their use and encourage gender sensitivity amongst both learners and teachers.

Online Learning: Indicators, for mapping and monitoring:

(Adapted from: *ENQA - Considerations for quality assurance of e-learning provision*, 2018)

INDICATORS
• Electronic security measures are considered by the institution's policy/code of practice.
• Collected data is used in order to evaluate e-learning programmes (e.g. comparative analysis of course design).
• There is a strategy on the use and purpose of learning analytics within the institution (i.e. the aim is improving student support).
• The information management system includes relevant, updated, and reliable information concerning the institution and its programmes.
• The institution considers ethical norms and government policy with respect to data protection and the privacy of students.