Document Name and Version	**10.1 Data Protection Policy**
Policy Number	10.1
Policies that Interact with Policy 10.1	10.2 Data Protection Processing Principles; 10.3 Data Management and Retention Policy; 10.4 Data Protection Subject Access Request (SAR) Policy; 10.5 Data Breach Policy; 10.6 Webpage Privacy and Cookie Notice; 10.7 Your Right of Access to Personal Information held by IICP College;
Approval Body	Board of Directors
Date of Approval	February 2020
Date Policy Comes into Force	25th January 2021
Date of Review	2025
Revisions	

1. **Preamble.**

1.1. IICP College (or the "College") needs to collect and use personal data for a variety of purposes relating to its employees, learners and other individuals who come into contact with the College.

1.2. Effective from 25th May 2018, the principle legislation governing data protection for all individuals within the European Union (EU) is the General Data Protection Regulation [GDPR]. The GDPR replaces previous Data Protection laws in the European Union. The GDPR gives living individuals greater control over their own personal data and places greater responsibility on those who collect, store retrieve and process data.

1.3. In addition to the GDPR, the following are also key legislative frameworks in force in relation to Data Protection[1]:

1.3.1. The Data Protection Act, 2018.

1.3.2. The Data Protection Acts, 1988 and 2003.

1.3.3. The 2011 "e-Privacy Regulations" (S.I. No. 336 of 2011 – the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011).

1.4. Personal data is any information that can identify an individual person. This includes a name, a postal address, online browsing history, images or anything relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

1.5. Organisations and businesses collecting and processing personal data are required by the GDPR to meet a very high standard in how they collect, use and protect data. In particular, organisations must always be fully transparent to individuals about how they are using and safeguarding personal data, and for how long they hold this data.

[1] For further information see Data Protection Commission (DPC) *Information on Key Data Protection legislative frameworks in this area*, available from: *https://www.dataprotection.ie/docs/legislation/k/1728.htm* (Accessed 27 October 2018).

This includes providing this information in easily accessible, concise, easy to understand and clear language.

1.6. All employees and learners who are dealing with personal data should ensure that they take reasonable measures to keep that data safe and secure. This includes ensuring that they are familiar with and adhere to IICP College's Data Protection policies. These include, in addition to this policy:

- Data Protection Processing Principles;
- Data Protection. Subject Access Request (SAR) Policy;
- Data retention and Retention Policy;
- Data Breach Policy.

1.7. The College also provides information to learners, staff and the public about its use of personal information. To this end it makes available the following documents:

- Data Protection in Assessments;
- Webpage Privacy and Cookie Notice;
- Data Subject Rights (DSR);
- Your Right of Access to Personal Information held by IICP College;
- How to make an Access Request (SAR).

1.8. The policies referred to in sections 1.6 and 1.7 above shall together be referred to as the "Related Policies".

2. Purpose.

2.1. The purpose of this policy is to state IICP College's commitment to protecting the rights and privacy of learners, staff and others in accordance with GDPR, and to outline principles for the classification, handling and administration of the data of IICP College in that regard.

2.1 This policy addresses the following legislative and regulatory requirements:

- General Data Protection Regulation [GDPR].

- QQI Sector-Specific Quality Assurance Guidelines for Independent/ Private Providers: Management of legislative and regulatory compliance.

3. Scope.

3.1. This policy applies to all areas and locations of IICP College and includes all areas of work of the College. This policy is equally applicable to records created and preserved in paper and electronic format.

3.2. This policy applies to all staff and learners of IICP College who collect and / or control the contents and use of personal data.

3.3. This policy relates specifically to Data Protection requirements. Personal data may also be subject to confidentiality, ethical, and security requirements, originating from legal, regulatory, professional or contractual obligations. Policies in relation to these areas are available in the College's Quality Assurance Manual [QAM].

4. Roles and Responsibilities:

4.1. The Board of Directors is responsible for formally approving this policy and for overseeing its implementation.

4.2. IICP College has overall responsibility for ensuring compliance with the GDPR. However, all employees who process personal data in the course of their employment are also responsible for ensuring compliance with the GDPR.

4.3. IICP College provides support, assistance, advice and training to appropriate individuals who are handling such data in order to ensure that they are in a position to comply with the legislation.

4.4. IICP College has appointed an individual as the point of contact for data protection issues in the College ("Data Protection Contact"). The Data Protection Contact's details are as follows:

Email: dataprotection@iicp.ie

4.5. The Data Protection Contact is responsible for the creation and implementation of associated policies and procedures, privacy notices, and developing and implementing Data retention and Retention Policy, in accordance with the latest legislation.

4.6. All members of staff are expected to acquaint themselves with and abide by the principles of GDPR as set out in this policy and its related policies. Please contact the Data Protection Contact in the event of any queries.

4.7. All staff have an obligation to report data protection breaches or contact the Data Protection Contact if they have concerns of such a breach. This will allow the appropriate personnel to investigate further and take the appropriate steps to fix the issue in a timely manner. Please refer to the Data Breach Policy for further information in this regard.

4.8. Staff will be supported and trained in the implementation of this and related policy. However, failure to comply with this policy or any of the Related Policies could have serious implications for the College, its staff and its learners. Consequently, failure of an individual staff member to comply may lead to disciplinary action, up to and including dismissal in accordance with the Disciplinary Procedures of IICP College.

4.9. All learners of the IICP Community are responsible for data protection in accordance with the academic regulations of IICP College.

5. **Definition of Terms.**

5.1. The following terms have specific legal meanings under the GDPR. The definitions given here are taken from the Data Protection Commissioner's *Rights of Individuals under the General Data Protection Regulation*[2] (available through: http://gdprandyou.ie/gdpr-for-individuals/).

[2] Data Protection Commission *Rights of Individuals under the General Data Protection Regulation* available through: http://gdprandyou.ie/gdpr-for-individuals/ (Accessed 27 October 2018).

5.2. Personal data

5.2.1. The term “personal data” means any information relating to a living person who is identified or identifiable (such a person is referred to as a “data subject”).

5.2.2. A person is identifiable if they can be identified directly or indirectly using an “identifier”. The GDPR gives examples of identifiers, including names, identification numbers, and location data. A person may also be identifiable by reference to factors which are specific to their identity, such as physical, genetic or cultural factors.

5.3. Processing

5.3.1. The term “processing” refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

5.4. Data Controller

5.4.1. A “data controller” refers to a person, company, or other body which determines the purposes and means of processing of personal data.

5.5. Data Processor

5.5.1. A “data processor” refers to a person, company, or other body which processes personal data on behalf of a data controller.

5.6. Profiling

5.6.1. Profiling is any kind of automated processing of personal data that involves analysing or predicting your behaviour, habits or interests.

5.7. Sensitive personal data

5.7.1. Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as “special categories” of personal data. The special categories are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or

trade union membership, as well as genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation. Processing of these special categories is prohibited, except in limited circumstances.

6. Policy.

6.1. IICP College holds and processes personal data about many different types of people such as its current, past or prospective employees, course applicants, learners, alumni, and members of the public. The College processes this personal data to carry out its educational, business and administrative functions and to comply with statutory requirements. This personal data is subject to the GDPR.

6.2. The GDPR is based on the core principles of Data Protection, which require organisations and individuals to:

- Collect no more data than is necessary from an individual for the purpose for which it will be used;
- Obtain personal data fairly from the individual by giving them notice of the collection and its specific purpose;
- Retain the data for no longer than is necessary for that specified purpose;
- Keep data safe and secure; and
- Provide an individual with a copy of his or her personal data if they request it.

6.3. Under the GDPR individuals have the significantly strengthened rights to:

- Obtain details about how their data is processed by an individual, organisation or business;
- Obtain copies of personal data that an organisation holds on them;
- Have incorrect or incomplete data corrected;
- Have their data erased by an organisation, where, for example, the organisation has no legitimate reason for retaining the data;
- Obtain their data from an organisation and to have that data transmitted to another organisation (data portability);

- Object to the processing of their data by an organisation in certain circumstances;
- Not to be subject to (with some exceptions) automated decision making, including profiling.

6.4. The GDPR places obligations on IICP College in relation to the way it handles personal data. In turn, the staff and learners of IICP College have responsibilities to ensure personal data is processed fairly, lawfully and securely. This means that Personal Data should be processed, secured, retained, disposed of and disclosed in accordance with the provisions set out in Section 6.2.

6.5. IICP College strives to include Privacy by Design and Privacy by Default principles in all its new services and business operations.

6.5.1. Privacy by Design means that each new service or business operation which processes personal data takes the protection of the data subject's personal data into consideration from the outset of the operation. [Please refer to our Data Protection Impact Assessment policy for further information].

6.5.2. Privacy by Default means that appropriate technical and organisational measures are in place for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

6.6. Types of personal data processed by IICP College.

6.6.1. The types of personal data processed by IICP College <u>in relation to staff</u> include:

- Title, name, address, contact details, email address, PPS number, date of birth, etc.;
- Original records of application, references, resumé, qualifications, transcripts, psychometric testing results, etc.;
- Record of appointments to promotion posts;
- Details of approved absences (sick leave, annual leave, career breaks, parental leave, study leave etc.);
- Details of work record;

- *Interaction details*: Engagement with IICP Staff, Moodle activity and use of facilities such as the library. Texts, emails and hard copy correspondence;
- *Online services:* IP address;
- *Garda Vetting Information*: Garda vetting documents may be required;
- *Other personal information:* Disciplinary information; images and voice recordings in assessments, records of any serious injuries/accidents and related matters; Details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress.

6.6.2. The types of personal data processed by IICP College <u>in relation to learners</u> include:

- *Personal details:* name, date of birth, country of birth, nationality, telephone numbers, addresses (home and term addresses), PPS number, gender, email address. The College may gather information such as car registration number, ID number, depending on specific circumstances.
- *Financial information*: Bank details including IBAN, BIC, name of bank/building society, credit card details (which are not retained), details of funding and fees paid and outstanding.
- *Information on others*: Next of kin/emergency contact details. The College may collect further information such as parents' socio-economic grouping, parents' occupation, parents' employment status depending on the circumstances.
- *Application Information:* Original records of application, references, resumé, qualifications, certificates, transcripts, personal statements and essay, and related data.
- *Academic information:* Academic history, academic grades, relevant work experience, exam scripts, continuous assessments, academic marks qualifications awarded, attendance record, library information and related data.
- Clinical information and materials: Clinical logs, personal therapy records and letters, professional body membership, insurance schedule, supervision

records, clinical readiness assessments, clinical placement forms, logs and reports, and related data.

- *Sensitive personal data:* Health and disability information, medical assessments, religion, ethnic origin, criminal convictions (for certain programmes which involve contact with minors). This sensitive personal data is collected to meet Government requirements, to monitor whether our equal opportunities policies are working and to ensure that learners with disabilities and other under-represented groups receive appropriate support. We are obliged to keep this special category of data as securely and as confidential as possible.
- *Interaction details*: Engagement with IT system, Moodle activity and use of facilities such as the library. Texts, emails and hard copy correspondence.
- *Online services:* IP address.
- *Garda Vetting Information*: Garda vetting documents.
- *Other personal information:* Disciplinary information; images and voice recordings in assessments, records of any serious injuries/accidents and related matters.

6.6.3. The types of personal data processed by IICP College through use of its website are set out in the IICP College *Privacy and Cookie Notice*.

6.7. IICP College will put in place a Data Register, which will identify the type of data held by IICP, and keep track of what happens to the data, including the basis for keeping it, how long it can be kept for and when it was deleted.

7. Procedures

7.1. IICP College has developed a range of policies and procedures in relation to information processing and management. These are intended:

7.1.1. To ensure compliance with its information management obligations, and

7.1.2. To communicate with data subjects using clear language.

7.2. Training:

7.2.1. Mandatory training will be provided to all staff on the GDPR.

7.2.2. Training will be provided to all new employees including temporary and contracted staff.

7.2.3. All employees will undertake refresher training on a regular basis.

7.3. IICP College has in place policies and procedures that guide the processing, securing, retention, disposal of and disclosure of personal data. All staff and learners are personally responsible for ensuring that they follow the procedures in place and seek further information if they are uncertain.

7.4. Data subjects have additional rights and individuals and organisations have additional responsibilities in relation to the processing of sensitive personal data. **Sensitive 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.

7.5. Personal data should only be *processed* if:

7.5.1. The College has a valid condition of processing, i.e.

- With the individual's unambiguous consent;
- Contractual obligation;
- In the legitimate interest of the data controller;
- In the vital interests of the data subject;
- In the public interest;
- In compliance with legal obligations.

7.6 Sensitive personal data should be treated with extra care. It should only be processed in accordance with the requirements set out in IICP College's *Data Protection Processing Principles*. In particular it should only be processed where at least one of the following conditions is satisfied:

- The data subject has given explicit consent; or

- The processing is necessary in order to exercise or perform a right or obligation which is conferred or imposed by law on the data controller in connection with employment; or
- The processing is necessary to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent; or
- The processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld; or
- The processing is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation; or
- The information being processed has been made public as a result of steps deliberately taken by the data subject; or
- The processing is necessary for the administration of justice; or
- The processing is necessary for the performance of a function conferred on a person by or under an enactment; or
- The processing is necessary for the performance of a function of the Government or a Minister of the Government; or
- The processing is necessary for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights; or
- The processing is necessary for medical purposes; or
- The processing is necessary in order to obtain information for use, subject to and in accordance with the Statistics Act, 1993; or
- The processing is necessary for the purpose of assessment of or payment of a tax liability; or
- The processing is necessary in relation to the administration of a Social Welfare scheme.

7.7 IICP College has in place *Data Protection Processing Principles* which restrict its processing of sensitive personal data to ensure that the GDPR restrictions on processing are adhered to.

7.7.1 The College provides information to the individuals concerned about how and why their information is being processed. In relation to website use, this is contained in the College website under *Webpage Privacy and Cookie Notice.*

7.7.2 The College is working towards ensuring that all required Privacy notices are in place.

7.8 Personal data should be *secured* in the following manner:

7.8.1 The data must be protected from inadvertent access, destruction, amendment or corruption.

7.8.2 Personal electronic data must be subject to appropriate security protection, such as passwords and encryption.

7.8.3 Screens and files showing personal data must not be visible to unauthorised persons.

7.8.4 Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.

7.8.5 Special care must be taken where laptops and personal computers containing personal data are used outside the College.

7.9 Personal Data should be *retained* subject to the following conditions:

- Data should not be kept for longer than is necessary for the purpose for which they were collected.
- Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose.

8.9.1 IICP College has in place a *Data retention and Retention Policy* which sets out the conditions of retention and destruction of personal data to ensure that the GDPR restrictions on retention are adhered to.

7.10 Personal Data should be *disposed of* subject to the following conditions:

7.10.1 Personal data should be disposed of when they are no longer needed for the purpose for which they were gathered.

7.10.2 Personal data should be disposed of in a manner that is appropriate to the sensitivity of the data.

7.10.3 IICP College has in place a *Data retention and Retention Policy* which sets out the conditions of retention and destruction of personal data to ensure that the GDPR conditions on destruction of personal data are adhered to.

7.11 Personal Data should only be *disclosed* subject to the following conditions:

7.11.1 Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept.

7.11.2 Any person disclosing information is required to satisfy themselves regarding the need to disclose.

7.11.3 Other than where there is a statutory or professional obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, no personal data will be disclosed without the consent of the data subject.

7.11.4 Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil administrative functions.

7.11.5 Personal data should not be disclosed outside of the EEA unless written consent has been obtained, unless disclosure is required for the performance of a contract to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

7.11.6 Permitted disclosures of personal data to a third party may occur where one or other of the following has been established:

- Disclosure of the data is authorised for safeguarding the security of the State;
- Data are required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- Data are required to protect the international relations of the State;

- Data are required urgently to prevent damage to health or serious loss/damage to property;
- Disclosure is required under law;
- Data are required for legal advice or legal proceedings;
- Disclosure occurs at the request or with the consent of the data subject.

7.11.7 The disclosure of **sensitive personal data** requires explicit consent in writing. Where there is a difficulty in obtaining written consent, verbal consent may be obtained by telephone in the case of **non-sensitive personal data**, but must include asking the subject to confirm facts that should be known only to them, such as date of birth, learner number, etc. The date and time of the giving of verbal consent should be recorded in writing.

7.12 *Data Subject Rights (DSR*). IICP College ensures that data subjects know their rights and how to enforce them. These rights are:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

7.12.1 A data subject has the right of access to personal data which has been collected concerning him or her by IICP College.

7.12.2 An application for access to data is called a Subject Access Request [SAR]. IICP College has in place a *Subject Access Request Policy* which sets out the conditions of Access to personal data to ensure that GDPR requirements are adhered to.

7.12.3 IICP College has in place information on the following in order to allow individuals to enforce their Data Protection Rights:

- Your Right of Access to Personal Information held by IICP College;
- How to make an Access Request (SAR).