TITLE: ***DATA PROTECTION POLICY***

Effective Date	19 January 2022	**Version**	4
			Major revision to simplify Policy; add DPIA template and ROPA; learners added to scope; changes made due to regulatory change and advices.
Approved By	Management Board	**Date Approved**	19 January 2022
		Review Date	19 January 2027 *or as required*
Superseded or Obsolete Policy / Procedure(s)		**Owner**	
See the Version Control Register on the last page.		Data Protection Officer (DPO)	

1. Purpose of Policy

Carlow College, St Patrick's (hereafter Carlow College) processes the personal data of employees, learners and other individuals with whom it comes into contact for a variety of purposes. Data Protection laws, including the General Data Protection Regulation (EU) 2016/679 (hereafter GDPR) and the Data Protection Acts 1988 to 2018 (which may be collectively hereafter referred to as Data Protection law), confer rights on individuals whose data is processed as well as responsibilities on organisations which process data. This Policy outlines Carlow College's responsibilities and the processes that are in place to comply with them.

This Policy is a statement of Carlow College's commitment to protect the data protection rights of individuals. Carlow College is committed to processing personal data in accordance with Data Protection law and the terms of this Policy.

2. Definitions

Controller means the natural or legal person, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Personal data means information relating to a living identified/identifiable natural person (**data subject**) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing means any operation performed on personal data, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Employees are not processors.

Special categories of personal data mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Criminal offence data does not fall within the scope of special categories of personal data but is subject to special protections.

3. Scope of Policy

All personal data, including special categories of personal data, created or received in the course of Carlow College business, in all formats, falls within the scope of this Policy. This Policy applies to all locations at which Carlow College personal data is processed, including remote working locations.

This Policy applies to:

- Any person who is employed or engaged by Carlow College, and who processes personal data in the course of their employment or engagement for administrative, academic, research or any other purpose;
- Any person who processes personal data in the course of their duties, including but not limited to, work placements or secondments;
- Individuals who are not directly employed by Carlow College, but who are employed by contractors, subcontractors or collaborative partners, and who process Carlow College personal data in the course of their duties;
- Any Carlow College learner who processes personal data for academic, administrative or any other purpose.

Hereafter, they may be collectively referred to as 'Members.'

4. Policy Statement

4.1 GDPR Principles

The GDPR sets out seven high-level principles to which controllers must comply when processing personal data. Failure to comply with the principles is a contravention of Data Protection law. This section describes the principles and provides summary information as to how Carlow College fulfils them. *Data Use and Security Guidelines* (Appendix 1) provide additional guidance for Members.

1	**Processed lawfully, fairly and in a way that is transparent to the data subject ('lawfulness, fairness and transparency')** Certain information must be given to data subjects about how their data is processed. Carlow College provides such information in Privacy Notices, which are available on the Data Protection section of the College website. Members are responsible for making Privacy Notices available to data subjects, where relevant: • Where information is collected directly from an individual, a Privacy Notice must be provided at the point at which data is collected e.g. when sending an application form for completion; not after the form is received; • Where information is obtained from another source, a Privacy Notice must be provided within one month of obtaining the data; • If personal data is used to communicate with the data subject, at the latest at the time of the first communication with the data subject; and if disclosure to another recipient is intended, at the latest when personal data is first disclosed. Privacy Notices are issued under the Data Protection Policy and the owner is the DPO. The DPO drafts and agrees Privacy Notices in consultation with relevant employees. Employees who require a new Privacy Notice should contact the DPO. Various College Policies describe how relevant personal data is processed. Members are to ensure they are familiar with Policies governing their work and activities. **Legal basis for processing** In order to process personal data lawfully, Carlow College must have a legal basis for doing so. GDPR Article 6 outlines six legal bases for processing: • Consent • Contract • Legal obligation • Vital interests • Public task • Legitimate interests Where special categories of personal data are processed, Carlow College must additionally identify a relevant legal basis as listed in GDPR Article 9. The legal bases that Carlow College relies on are outlined in the Records of Processing Activities (ROPA) (see Appendix 2). **Consent** • Consent is a well-known legal basis for processing personal data. Consent must meet specific criteria in order to be valid, including that it is freely given, specific and unambiguous. Consent may also be later withdrawn.

	• It may not be appropriate to use consent in some circumstances, for example, if there is an unequal relationship between controller and data subject e.g. College and employee or learner. • Any proposed use of consent beyond that set out in the ROPA must be discussed in advance with the DPO. • Any employee who requires a consent form should contact the DPO. Such forms must be worded and structured in a specific manner in order for consent to be valid. • A record of consent must exist e.g. a written record or recorded oral statement. • Employees are not to share consent forms. Forms created for one purpose may not be appropriate in another context.
2	**Collected for a specified, explicit and legitimate purposes and not further processed in an incompatible manner ('purpose limitation')** Carlow College only collects and otherwise processes data for purposes that are clearly stated, specific and lawful. Such information is given in Privacy Notices, and College Policies provide additional information about how personal data may be used. Data should not be reused for additional purposes and in ways that would not be expected by data subjects.
3	**Adequate, relevant and limited to what is necessary ('data minimisation')** The minimum personal data needed to carry out a purpose should be collected and processed. The data that is processed is reviewed periodically in order to comply with this requirement. Personal data should be shared both internally (e.g. among staff) and externally only when required. Particular attention should be paid to special categories of personal data, the disclosure sometimes requires explicit consent. In some cases, it may be possible to fulfil a purpose without collecting personal data (e.g. permitting anonymous responses to surveys).
4	**Accurate and, where necessary, kept up to date ('accuracy')** Carlow College seeks to ensure that data that it processes is complete, accurate and up to date. The College takes reasonable steps to ensure that data is recorded accurately or is rectified or erased, as appropriate, if it is found to be inaccurate.
5	**Kept in a form that permits the identification of data subjects for no longer than is necessary ('storage limitation')** The GDPR provides that personal data should not be kept in a form which allows identification of data subjects for longer than is necessary. Records Retention Schedules form part of the College's Records Management Policy. Records Retention Schedule advise employees on retention periods for both personal data and non-personal records. Personal data may be stored for longer periods if it is processed solely for archiving in the public interest, scientific or historical research purposes or statistical purposes, subject to safeguards. Carlow College's archival records are managed by the Delany Archive Trust, which has a suite of policies in place to safeguard personal data.

6	**Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')** Access to Carlow College's manual and IT systems is subject to security and acceptable use policies which outline the responsibilities of those using the systems. See Appendix 1 for *Data Use and Security Guidelines*, with which Members are to comply.
7	**Finally, the controller must be able to demonstrate compliance with principles 1-6 ('accountability')** Carlow College keeps various records to demonstrate compliance with these principles. <u>Records of Processing Activities (ROPA)</u> This comprises an inventory of personal data processed by Carlow College and includes reference to the relevant legal basis for processing the data (see Appendix 2). It is coordinated by the DPO. Managers are responsible for reviewing the inventory periodically in respect of their remits, certifying that it is accurate and notifying the DPO of any required changes. <u>Privacy by Design and Default</u> Two key principles of Data Protection law are privacy by design and by default. Privacy by design means that activities that involve processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, policy development and IT systems. In practice, this means that the College must ensure that data protection is considered from the design stage of activities. Employees are responsible for ensuring that the DPO is involved from an early stage in any process or project that involves personal data processing. Carlow College ensures privacy by design and by default by various means, including the provision of training and Data Protection Impact Assessments.

4.2 Training

Carlow College aims to ensure that employees and learners who process personal data as part of their roles have awareness of, and when necessary, receive training relating to Data Protection principles and law, and Carlow College practices.

4.3 Sharing Data with Third Parties

4.3.1 Processors

A processor is a third party that processes personal data on behalf of a controller. Processors have access to personal data in the context of providing a service. This can be very varied and includes, for example, software providers, online account providers and CCTV monitoring companies.

Prior to engaging processors, Carlow College:

- Undertakes due diligence to ensure that it is appropriate to engage the processor;
- Puts in place an agreement with the processor that meets the requirements of Data Protection law.

When a controller contracts a processor, it is the controller's responsibility to ensure that Data Protection contract clauses are in place to protect the data. Notwithstanding this, many processors supply Data Protection contract clauses to controllers for review. Data Protection clauses may be a stand alone document or part of a larger agreement.

Employees who receive Data Protection contract clauses from processors are to send them to the DPO prior to agreeing a contract. This includes contracts of all types, for example, formal contracts as well as terms and conditions or terms of service for online accounts.

Carlow College has a template Data Processing Agreement (Appendix 3), which may be used when Carlow College needs to provide Data Protection contract clauses. Employees are to contact the DPO prior to providing a Data Processing Agreement to any third party.

Review section 4.3.3, entitled 'Transfers of Personal Data outside of the European Union (EU),' if it is proposed to transfer personal data outside of the EU.

4.3.2 Data Sharing Agreements / Joint Controller Agreements

It may be necessary to agree data sharing or joint controller agreements with third parties on some occasions, for example, an organisation being partnered with on a project. Third parties may be joint or independent controllers. Employees should contact the DPO at an early stage in discussions with external parties if it is anticipated that personal data will be shared. Any agreement received from a third party should be sent to the DPO for review prior to execution.

Review the section entitled 'Transfers of Personal Data outside of the European Union (EU)' if it is proposed to transfer personal data outside of the EU.

4.3.3 Transfers of Personal Data outside of the European Union (EU)

The GDPR imposes restrictions on the transfer of personal data outside of the EU. These restrictions are in place to ensure that the level of protection afforded by the GDPR is not undermined. Employees are to contact the DPO if they intend to transfer personal data outside of the EU.

Transfers may proceed where the European Commission has decided that a third country, a territory or one or more sectors in the third country, or an international organisation ensures an adequate level of data protection. The European Commission has issued 'adequacy decisions' in respect of a number of countries, which means that the country is adjudged to provide an adequate level of data protection.[1] Transfer Impact Assessments will be carried out by the DPO in conjunction with relevant employees where it is proposed to transfer personal data to third countries where an 'adequacy decision' is not in place.

Some other mechanisms for data transfer include, but are not limited to:

- The data subject has explicitly consented to the transfer, after having been informed of the possible risks of the transfer for the data subject due to the absence of an adequacy

[1] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, [accessed 25 May 2021].

decision. Any employee who proposes to transfer data to a third country for individual data subjects is responsible for acquiring consent.

- An agreement incorporating Standard Contractual Clauses approved by the EU Commission.
- Binding corporate rules.

4.4 Data Subject Rights

Data subjects have a number of data protection rights, as outlined in the following table. These rights are subject to certain exemptions.

Right	**Explanation**
Information	To receive information about how data is used
Access	To receive a copy of data that is processed
Rectification	To have incomplete or incorrect data corrected
Erasure	To have data deleted, also known as the 'right to be forgotten'
Restriction of processing	To limit the way that data is used
Data portability	To transfer data to another controller
Objection	To object to how data is processed
Rights in relation to automated decision making and profiling	The right not to be subject to wholly automated processing, which produces legal or other significant effects for the data subject

In general, data subject requests must be replied to within one month and are free of charge.

Access requests should be sent to the DPO without delay. The DPO will reply on behalf of the College, consulting with employees as required and taking legislative exemptions into account. Other types of requests should be notified to the DPO without delay and the DPO will assist employees in responding to requests.

No particular form is prescribed in the GDPR for data subject requests, so they may be verbal or written, and they need not mention data protection or GDPR. The *Data Subject Request Form* (Appendix 4) is made available on the College website but its use is not obligatory.

*4.5 Data Protection Impact Assessment (DPIA***)**

A DPIA is an exercise that helps to identify and mitigate or eliminate data protection risks of a project.

Under the GDPR, it is mandatory to carry out a DPIA if there is a high risk to data subjects. Some non-exhaustive examples are provided by the GDPR:

- Systematic and extensive profiling with significant effects.
- Processes special category or criminal offence data on a large scale.

- Systematically monitors publicly accessible areas (e.g. CCTV).

The Data Protection Commission (DPC) has prescribed additional areas where DPIAs are mandatory. These include, but are not limited to:

- Profiling vulnerable persons, including children to target marketing or online services at such persons.
- Systematically monitoring, tracking or observing individuals' location or behaviour.
- Processing biometric data to uniquely identity or authenticate the identity of individuals.
- Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the datasets are combined from different sources where processing was/is conducted for different purposes or by different controllers.

A DPIA should be conducted before data processing begins, and commence as early as possible during a project's design stage. DPIAs are 'live' documents so if the nature or scope of the data processing changes, the DPIA should be updated.

Even if it is not mandatory, it is good practice to conduct a DPIA and it may help to structure thinking about a project. Not all risks can be eliminated, but a DPIA can allow data protection risks to be identified and mitigated, plan for implementation of solutions, and assess the viability of a project at an early stage. If a DPIA does not identify mitigating safeguards against residual high risks, the DPC must be consulted.

DPIAs are the responsibility of the project team. Under GDPR Article 35, it is necessary to seek the advice of the DPO. The DPO should be made aware of the project at an early stage and be involved by the project team throughout.

Detailed information is available from the DPC about when a DPIA is required and how to conduct the exercise.[2] A DPIA template is available at Appendix 5.[3]

4.6 CCTV

Use of CCTV must comply with Data Protection law. Carlow College uses CCTV in accordance with its CCTV Policy. Installation of CCTV is subject to a DPIA.

4.7 Covert Recording and Surveillance

This refers to recording, audio or visual, carried out without the knowledge and consent of an individual(s). It includes devices and systems of all types, including but not limited to, CCTV, phones and virtual meeting platforms.

Covert surveillance is generally unlawful and is normally permitted only on an exceptional case-by-case basis where data is kept for purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This implies involvement of An Garda Síochána or other prosecution authorities. Any covert surveillance conducted by Carlow

[2] https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#:~:text=A%20Data%20Protection%20Impact%20Assessment%20(DPIA)%20describes%20a%20process%20designed,demonstrating%20compliance%20with%20the%20GDPR [accessed 25 May 2021].
[3] https://www.dataprotection.ie/sites/default/files/uploads/2019-05/CCTV%20guidance%20data%20controllers_0.pdf [accessed 18 May 2021].

College will be approved by a representative group of senior management and comply with standards set out by the DPC.4

Employees and learners are not permitted to carry out covert recording of employees, learners or any person with whom they come into contact in the workplace or through the course of their duties or studies. Unauthorised covert recording undermines trust and confidence and can contravene the 'fairness, lawfulness and transparency' principle of the GDPR.

4.8 Marketing

It is intended to put a Guide to Direct Marketing in place. Unsolicited direct marketing is one of the main sources of complaint by individuals to the DPC.

The ePrivacy Regulations (SI 336 of 2011) sit alongside other Data Protection laws, and the forthcoming Guide to Direct Marketing will focus on all applicable legislation. The ePrivacy Regulations give people specific rights in relation to electronic communications and contain rules on:

- Marketing communications, such as calls, emails and text messages.
- Cookies and similar technologies.

4.9 Children's Personal Data

- Children, who are defined as being under the age of 18, need particular protection when their personal data is processed as they may be less aware of the risks involved.
- Some learners and other individuals (e.g. attendees at Student Recruitment events) who engage with Carlow College are under the age of eighteen. Where new processes using the personal data of individuals under eighteen are proposed, they should be brought to the attention of the DPO to ensure suitability.
- Employees should be mindful of any law, statutory guidance or best practice etc that concerns children (e.g. those providing counselling to minors must secure advance parental consent).
- Information, such as Privacy Notices, must be written in a manner that it can be understood by children.
- If consent is the lawful basis for processing personal data when offering an online service directly to a child, only children aged 16 or over can provide their own consent.
- For children under this age, consent needs to be obtained from whomever holds parental responsibility, unless the service is a preventive or counselling service.
- Children have specific protections when their data is used for marketing purposes or creating user profiles.
- Children have the same data protection rights as adults and their right to erasure is enhanced if they gave consent to processing as a child.

4.10 Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

It is important to understand that a personal data breach can happen within an organisation (e.g. personal data shared inappropriately among employees) as well as involving an external person or organisation.

Any employee who is aware of an actual or suspected personal data breach or incident by Carlow College is to contact the DPO immediately. Incidents of data being placed at risk should also be notified to the DPO as they may be lessons that can be learned. If it is not possible to contact the DPO, employees are to contact the President's Office or Director of Operations.

Any employee who is notified of a personal data breach by a processor, joint controller or other collaborative party is to notify the DPO immediately.

Data breaches are assessed and responded to as described in the *Personal Data Breach Response Plan* (see Appendix 6).

Where any employee or learner mistakenly receives personal data, the following steps are also to be taken to reduce risks to the rights of the data subject:

- Avoid opening email attachments, files or other documents that are not yours to open.
- Identify the controller (e.g. from the sender's email address or letterhead) and inform them of the mistaken disclosure. Do not wait for the sender to contact you. If you require assistance, you can contact Carlow College's DPO but do not send the breached data.
- Agree with the controller how to resolve the mistake. This will depend on the circumstances e.g., you may be asked to permanently delete an email (by deleting it from your 'inbox' and 'deleted items' folder) or securely destroy a paper item, and confirm to the controller that you have carried out the agreed action.
- Do not attempt to identify or contact the person the data is about as this is further processing the data.
- Do not share the data with another third party, including publicly uploading the data to social media platforms.

4.11 Pseudonymised and anonymised data

Pseudonymised data is data from which direct identifiers have been removed, but as it is possible to re-identify individuals, it is personal data. Anonymised and anonymous information, from which it is not possible to identify individuals, is not personal data.

The DPC has published a guidance note on anonymisation and pseudonymisation.[5] Employees and learners should familiarise themselves with the guidance note and ensure that they use these terms correctly when describing data.

[5] Data Protection Commission Guidance on Anonymisation and Pseudonymisation, https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf [accessed 25 May 2021].

4.12 Online meetings and events

Guidelines are provided in Appendix 7.

5. Roles and Responsibilities

Carlow College has overall responsibility for complying with this Policy and Data Protection Law.

Employees, learners and other Members:

- Must comply with this Policy and Data Protection law.
- Must cooperate with the DPO.
- Must complete training and awareness activities provided by the College.
- Should take all necessary steps to ensure that no personal data breaches result from their actions.
- Must report all suspected and actual personal data breaches and incidents, and data being placed at risk, to the DPO immediately.

Failure to adhere to this Policy may result in disciplinary action as set out in the Staff Disciplinary Policy and the Learner Code of Conduct and Disciplinary Policy.

Managers are responsible for:

- Ensuring compliance with this Policy in their respective areas of responsibility.
- Cooperating with the DPO on keeping the ROPA up to date.

Programme Directors are responsible for ensuring that where learners process personal data as part of their programmes of studies, they receive adequate information/training to permit them to comply with this Policy.

The **DPO** is responsible for:

- Informing and advising Carlow College and its employees of their obligations pursuant to Data Protection law.
- Monitoring compliance with Data Protection law and Carlow College Policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff, and related audits.
- Providing advice, where requested, as regards DPIAs and monitoring their performance;
- Cooperating with and acting as the contact point for the DPC.
- Maintaining records of personal data breaches.
- Responding to and assisting with data subject requests.
- Coordinating the ROPA.

6. Associated Documentation

Appendix 1	Data Use and Security Guidelines
Appendix 2	Records of Processing Activities (ROPA)
Appendix 3	Template Data Processing Agreement
Appendix 4	Data Subject Request Form
Appendix 5	Template Data Protection Impact Assessment
Appendix 6	Personal Data Breach Response Plan
Appendix 7	Online Meetings and Events
Appendix 8	Privacy Notices

7. Referenced Policies

- *CCTV Policy*
- *Disciplinary Policy (Staff)*
- *Learner Code of Conduct and Disciplinary Policy*
- *Records Management Policy*

8. Monitoring and Review

This policy is reviewed every three years, or more frequently, if required by legislative or regulatory change.

Version Control Register

Version No.	Superseded or Obsolete Policy / Procedure(s)	Date Approved	Changes
1	*Data Protection Policy*	17 April 2014	Initial Issue
2	*Data Protection Policy*	25 April 2015	Policy revised to respond to employee questions and provide clarity.
3	*Data Protection Policy*	23 May 2018	Major revision to coincide with the advent of the GDPR.
3.1	*Data Protection Policy*	8 April 2020	Minor changes to reflect the enacted *Data Protection Act 201*8 and new guidance documentation.
4	*Data Protection Policy*	19 January 2022	Major revision to simplify Policy; add DPIA template and ROPA; learners

			added to scope; changes made due to regulatory change and advices.