Contents

1 Data Protection Policy

1.1.1 Policy Owner

The policy owner is the Board of Directors.

1.1.2 Purpose

This policy aims to provide information and transparency regarding the Data Protection obligations of Cenit College to comply with all applicable Data Protection Regulations, including the EU General Data Protection Regulation (GDPR), the Data Protection Acts 1988 to 2018 and the ePrivacy Regulations 2011.

It applies to all processing of personal data undertaken by Cenit College relating to employees, learners, and other stakeholders. When processing personal data Cenit College complies with data protection legislation guided by the GDPR data protection principles to ensure that data is:

- Processed fairly, lawfully and in a transparent manner
- Used only for limited, specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary
- Accurate and, where necessary, up to date
- Not kept for longer than necessary; and
- Kept safe and secure.

See Appendix A for a summary of the lawful bases for processing and data subject rights.

1.1.3 Scope

This policy applies to processing activities concerning personal and sensitive data carried out by Cenit College in the normal course of its business.

Specifically, this policy applies to:

- Any individual who receives, handles, or processes personal data on behalf of Cenit College. This cohort includes direct employees (full and part-time), tutors, etc.
- Third-party organisations that receive, handle or process personal data on behalf of Cenit College. This cohort is often referred to as a data processor or sub-processor.

This Policy should be read in conjunction with

Privacy Notice - Cenit College

1.1.4 Responsibilities

The following personnel are responsible for Data Management within Cenit College.

Role	**Responsibility**
Board of Directors	Overall responsibility for Data Management within Cenit College.
Management Committee	Responsibility to execute the policy.
Head of Finance	Maintaining all financial records
Staff	ensuring compliance in their respective roles and duties.
Director of Digital and Technology	• maintaining our server where data is held i.e., security, configuration and maintenance. • Back-up(s) • VLE and storage of data

	• Monitor the IT environment and perform regular maintenance checks
Head of Training	Responsible for preparing reports
Examinations Officer	Transferring results into the awarding body's system
Quality Manager	Responsible for all data concerning the quality assurance of Cenit College's activities.
Data Protection Manager (DPM)	We have appointed a Data Protection Manager who has the following responsibilities: • to inform and advise Cenit College and the employees who carry out processing of their obligations according to Irish data protection legislation, including EU GDPR. • Monitor compliance with the GDPR, other data protection legislation, and the policies of Cenit College concerning the protection of personal data, including the assignment of responsibilities, awareness-raising, and training of staff involved in processing operations, as well as related audits. • To provide advice, where requested, as regards data protection impact assessment (DPIA) and to monitor their performance according to Article 35 of the GDPR. • To cooperate with the Office of the Data Protection Commissioner. • To act as a contact point for the Office of the Data Protection Commissioner on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, regarding any other matter. • To liaise with the Office of the Data Protection Commissioner regarding personal data breaches, complaints or requests • In performing their tasks, they consider the risk associated with processing operations and the nature, scope, context, and purposes of processing.

1.1.5 Policy Statement

Cenit College processes and stores data about the following.

- Learners
- Employees
- Past employees
- Applicants (employment and learners)
- Service providers

Cenit College ensures that personal data is processed according to EU and National legislation and is committed to carrying out this legislative requirement within its organisation. This policy and associated procedures, controls and measures ensure that all Cenit College employees and contractors are fully aware of their data protection responsibilities, including advising the DPM of any data breach, potential data breach, data subjects rights request or data protection enquiry.

Should any staff member of Cenit College fail to process Personal Data in compliance with this policy, disciplinary proceedings may be initiated against them.

1.1.6 Data Protection Contact (Complaints and Enquiries)

All personal data enquiries should be made to the Cenit College DPM at the following email address: dataprotection@cenitcollege.ie

1.1.7 Rights of the Data Subject

Under GDPR, individuals have the following rights:

1. Right to be Informed. Data subjects should be informed about the collection and use of their personal data at time of collection.
2. Right of Access. Data subjects can request a copy of their personal data and details on how it is being processed.
3. Right to Rectification. Data subjects can ask for inaccurate or incomplete personal data to be corrected.
4. Right to Erasure (Right to be Forgotten). Data subjects can request deletion of their data in certain circumstances, such as when it's no longer needed or processed unlawfully.
5. Right to Restrict Processing. Data subjects can limit how their data is used, for example, while accuracy is being verified.
6. Right to Data Portability. Data subjects can ask for and receive their data in a structured, commonly used format and transfer it to another controller.
7. Right to Object. Data subjects can object to processing based on legitimate interests, direct marketing, or tasks carried out in the public interest.
8. Right not to be subject to a decision based solely on automated processing.
9. Withdraw consent, where consent is the legal basis for data processing.

An overview of these rights is provided in Appendix A, including the legal basis under Articles 12–23 of the GDPR

1.1.8 Consent for Data Processing

Under Article 7 of the GDPR legislation, where processing is based on consent, Cenit College will demonstrate that the data subject has consented to processing their personal data. Where consent is given by the data subject (for example, the use of personal data for marketing purposes), Cenit College obtains this consent in writing. Such consent must be clearly presented, freely given and in a form that uses clear and plain language.

Such consent can be withdrawn at any time by the data subject. However, the withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this.

Cenit College will ensure that the following protocols are implemented regarding consent.

- Consent will be documented in writing, including the date and the specific information provided at the time consent was obtained, along with what the data subject was told when the consent was given.
- Data Subjects are asked to 'opt in'- no prefilled boxes should be displayed.
- Clear and plain language should be used on all forms and information sources.
- Data Subjects will be informed, at the point of giving consent, how to change their preferences. It will be as easy to withdraw as to give consent.
- The purpose for which the data is collected is explicit and lawful.
- Consent should be periodically reviewed to ensure currency and the legitimacy of purpose.

For a breakdown of the conditions for valid consent under Article 7 GDPR, refer to Appendix A.

1.1.9 Third-Party Processors

As a Data Controller, Cenit College may contract a third party to process Personal Data on its behalf. In such circumstances, a written contract will be established with the third party, clearly outlining their obligations regarding the processing of Personal Data, in compliance with EU GDPR practices. Cenit College will remain the Data Controller and is ultimately responsible for how the data will be used.

A formal **Data Processing Agreement (DPA)** will be established for each relationship to document the terms of processing, responsibilities, and safeguards under GDPR requirements.

Should a Data Processor fail to manage Cenit College's data in a compliant manner, this will be viewed as a breach of contract and may result in recourse to the legal system.

1.1.10 Joint Data Controllers

Cenit College may act as a Joint Data Controller in certain circumstances, sharing responsibility for processing personal data with other organisations. Each joint controller must clearly define and document their respective responsibilities for compliance with GDPR, including transparency obligations and mechanisms for data subject rights.

In such cases, Cenit College and the partner organisation will jointly determine how to process personal data. Each party is independently responsible for ensuring that personal data is collected, processed, retained, and shared in compliance with the General Data Protection Regulation (GDPR).

Regardless of whether Cenit College is acting as a sole or joint Data Controller, data subjects retain the right to exercise their GDPR rights directly with Cenit College. All joint controllers are required to uphold these rights in full.

A formal **Data Sharing Agreement (DSA)** will be established for each relationship to document the terms of processing, responsibilities, and safeguards under GDPR requirements. See Appendix A for lawful bases and responsibilities under joint controller arrangements, particularly Article 6 and Article 26 GDPR.

1.1.11 Cenit College as a Data Processor

In certain circumstances, Cenit College may act as a data processor, processing personal data for another organisation (the data controller). This typically arises when delivering training, assessments, or other services funded or commissioned by external partners, such as corporate clients, government agencies, or education bodies.

Where Cenit College acts as a Data Processor, it does not determine the purpose or means of processing personal data but follows the Data Controller's documented instructions.

In such arrangements, Cenit College is committed to fulfilling its obligations under Article 28 of the GDPR. These obligations include:

- **Processing personal data only on documented instructions** from the Data Controller, including transfers to third countries or international organisations, unless required by EU or Member State law.
- **Implementing appropriate technical and organisational security measures** to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- **Ensuring staff members are bound by confidentiality** and are trained on their data protection responsibilities.
- **Assisting the Data Controller** in fulfilling its obligations, particularly regarding:

- Data Subject Access Requests (SARs)
- Data Protection Impact Assessments (DPIAs)
- Incident and breach notification

- **Do not engage any sub-processors without prior written authorisation of the Data Controller and ensure** equivalent data protection obligations are imposed on any sub-processor.
- **Deleting or returning personal data** to the Data Controller upon completion of services, unless required by law to retain it.
- **Maintaining a written record of processing activities** carried out on behalf of each Data Controller.

Where Cenit College is unsure of any instruction provided by the Data Controller or considers that an instruction may breach GDPR or other applicable data protection laws, it will immediately seek clarification before proceeding.

A formal **Data Processing Agreement (DPA)** will be established for each relationship to document the terms of processing, responsibilities, and safeguards under GDPR requirements.

1.1.12 Data Collection Principles

In the course of its daily organisational activities, Cenit College acquires, processes, and stores personal data in relation to:

- Learners
- Employees
- Past employees
- Contracted Staff
- Applicants (employment and learners)
- Service providers

Under Cenit College's GDPR policy, this data must be acquired and managed fairly and lawfully. Cenit College is committed to ensuring all staff members are aware of GDPR and are required to complete mandatory GDPR training each year.

Cenit College ensures that all data is:

1. *Processed lawfully, fairly and in a transparent manner in relation to the data subject.* Cenit College will always safeguard the rights and freedoms of the data subjects. The processing of data will be achieved in the following manner.
    a. The data collected must be justified, i.e., legally, contractually necessary, etc., and collected as part of Cenit College's lawful activities.
    b. Where applicable hrough informed consent from the data subject.
    c. Where CCTV is installed on our premises, we ensure that the appropriate signage is displayed to ensure transparency.
    d. Where CCTV is used, this information is used transparently.
    e. Cenit College will only share personal information with third parties if we are under a duty to disclose, or to comply with any legal, contractual or regulatory obligation or request, including any safeguarding concerns.

2. *Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be*

considered to be incompatible with the initial purposes; Cenit College will fulfil this obligation by:

a. Only obtaining data for specific, lawful, and clearly stated purposes.
b. Cenit College will clearly state the purpose for the data processing.
c. Allow the Data Subject the right to question the purpose(s) for which Cenit College holds their data.

3. *Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.* Cenit College will fulfil this obligation by ensuring that only the personal data necessary for the purpose will be collected and its usage of the data will be compatible with the purposes for which the data was acquired.
4. *Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.* Cenit College will fulfil this obligation by*;*
    a. Ensuring that data accuracy and access are regularly assessed through defined mechanisms, such as audits and administrative and IT validation processes.
    b. Conducting periodic reviews and audits to ensure that relevant data is kept accurate and current.
    c. Ensuring that the data subjects have the means to verify the accuracy, currency and completeness of their personal data and are afforded the opportunity for correction action if required.
5. *Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject*. Cenit College will fulfil this obligation by*.*
    a. Developing a data management records retention policy (refer to policy 8.2 Information Management Policy) that outlines personal data retention periods. This retention period will be based on the purpose of data collection, the lawful basis for processing and contractual/legal requirements. This will be published by Cenit College and strictly implemented.
    b. Undertaking regular audits to ensure full compliance with the records retention policy.
    c. Training staff in their responsibilities and obligations regarding the retention of personal data.
    d. Developing and implementing a policy that addresses the measures for the secure destruction, deletion or archiving of personal data at the end of the retention period.
6. *Processed to ensure 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.* Cenit College will fulfil this obligation by*.*
    a. Employing appropriate security standards to protect any personal data they hold. This included measures to protect against unauthorised access, alteration, or destruction of such data.
    b. Ensure that staff are trained to know their obligations and responsibilities regarding personal data.

c. Ensuring that access and management of personal data is only accessible by permitted staff members with the given authorisation and password access that is reviewed and changed periodically.

7. *The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle").* Cenit College will fulfil this obligation by:
   a. Appointing a DPM to ensure that all data records are adequately maintained, managed, and secured. The DPM will assist with the completion of data impact assessments where appropriate. Additionally, they will ensure that contracts with processors acting on their behalf, detail their processing obligations.
   b. Devising internal policies and a code of conduct, reporting data breaches (Refer to our Data Breach policy), and implementing privacy policies.
   c. Carrying out periodic reviews of its accountability measures.
   d. Complying with other principles (which will assist accountability) such as implementing appropriate technical and organisational measures, having concise, accessible, transparent information, and having clear record retention policies.

The principles outlined here are further supported by GDPR Articles 5 and 6, summarised in Appendix A.

1.1.13 Data Subjects Access Requests

Data subject access requests (for information regarding Data Subject Access Requests refer to the QA8.4 Data Subjects Access Request Policy), are processed promptly and responded to within 30 days from date of receipt. If the college is acting as a processor, the request will be referred to the relevant controller for processing.

Cenit College will confirm the identity of the requester before processing the request, and where necessary will require a photocopy of an official document, such as Passport plus a copy of a recent utility bill showing the requestor's current address.

Cenit College may also withhold personal information requested to the extent that it is permitted by legislation.

If a data subject is not satisfied with the information provided by Cenit College or they believe that their rights as a data subject have not been addressed, they can make a formal complaint to the Data Protection Commissioners (Ireland), who can be contacted as follows.

- Post: Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, R32 AP23, Ireland.
- Phone: +353 (0761) 104800, or
- Email: info@dataprotection.ie

1.1.14 Data Protection Impact Assessments (DPIA)

Article 35 of the GDPR legislation states that *where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

Cenit College will carry out a DPIA when the processing presents or could present a high risk to the rights and freedoms of the data subjects. GDPR recommends a DPIA in the following circumstances:

1. Processing of large amounts of personal data
2. Processing of special categories of personal data
3. Where there is automated processing or profiling
4. Systematic monitoring
5. Evaluation and Scoring (including profiling and predicting)
6. Matching or combining data sets (originating from more than one data processing operation)
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. Data transfer across borders outside the European Union
10. When the processing itself 'prevents data subjects from exercising a right or using a service or a contract'

Cenit Colleges' DPIA will include the following.

1. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.
2. An assessment of the necessity and proportionality of the processing operations concerning the purposes.
3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
4. The measures envisaged to address the risks include safeguards, security measures, and mechanisms to ensure personal data protection and demonstrate compliance with the GDPR Regulation, considering the rights and legitimate interests of data subjects and other persons concerned.

Cenit College will review DPIA's to continue to monitor risks and mitigations. See Appendix A for DPIA requirements and risk assessment criteria under Article 35 GDPR.

1.1.15 Special Categories of Personal Data

Under Article 9 of the GDPR, Cenit College recognises that special categories of personal data identifying racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation require additional protection. Processing of such data is subject to stricter conditions and safeguards. For a complete list of special categories and lawful conditions for processing under Article 9 GDPR, refer to Appendix A.

1.1.16 Monitoring of this Policy

The QA Manager will monitor this policy as part of their annual quality audit to ensure the currency and relevance of this policy.

In conjunction with the Board of Directors, the DPM will continuously monitor and approve this policy using the following mechanisms.

- Review of data protection enquiries, complaints, requests, breaches, withdrawals of consent.
- Integration with other policies such as Privacy Notice, Data Subject Rights/Access procedure, Records Retention schedule (Refer to policy 8.2).

2 Version Control and Classification

2.1 Version

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	11/08/2020	Perri Williams (QA)	New QA system
2	23/03/2021	Perri Williams (QA)	Management review: Revisions for grammar and spelling
3	28/08/2023	Barbara Forde (DPM)	General Review to ensure compliance
4	22/11/2023	Judy De Castro (Commsec)	General Review to ensure compliance, minor changes
5	08/05/2025	KMCD	Check over and added a section on Cenit College as a processor.
6	15/10/2025	BF (DPM)	Updated to be in line with UK version. Updated list of rights for data subjects Added to list of where DPIA's are required Slight rewording of some paragraphs 1.1.10 – typo – changed DPA to DSA

2.2 Classification

**Use the information fields in MS Word to auto-update these fields.*

DOCUMENT CLASSIFICATION	Internal
PRINTING	Uncontrolled when printed
DOCUMENT REF	QA 8.3
VERSION	5
LAST APPROVAL DATE	15/10/2025

Appendix A: Summary of Key GDPR Provisions

i. Lawful Bases for Processing (Article 6 GDPR)

Personal data must be processed lawfully, fairly, and transparently. The lawful bases include:

1. **Consent** – The individual has given explicit permission.
2. **Contract** – Processing is necessary for a contract with the individual.
3. **Legal Obligation** – Required to comply with the law.
4. **Vital Interests** – To protect someone's life.
5. **Public Task** – Necessary for official functions or public interest.
6. **Legitimate Interests** – Necessary for your legitimate interests or those of a third party, unless overridden by the individual's rights.

ii. Conditions for Consent (Article 7 GDPR)

Consent must be:

- Freely given, specific, informed, and unambiguous.
- Clearly distinguishable from other matters.
- Easy to withdraw at any time.
- Documented as evidence of compliance.

iii. Special Categories of Personal Data (Article 9 GDPR)

These include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Health data
- Data concerning sex life or sexual orientation

Processing is prohibited unless:

- Explicit consent is obtained
- It's necessary for employment, social protection, or legal claims
- It's in the public interest or for health/public health purposes

iv. Data Subject Rights (Articles 12–23 GDPR)

Individuals have the right to:

Be informed about how their data is used

- **Access** – their personal data
- **Rectification** - of inaccurate or incomplete data
- **Erasure** – "right to be forgotten"
- **Restrict processing** – under certain conditions
- **Data portability** – transfer data to another provider
- **Object** – to processing based on legitimate interests or direct marketing
- **Not be subject to automated decision-making** - including profiling

v. Data Protection Impact Assessments (DPIAs) (Article 35 GDPR)

Required when processing is likely to result in a high risk to individuals' rights and freedoms. DPIAs must:

- Describe the processing and its purpose
- Assess necessity and proportionality
- Identify and mitigate risks