

Contents

1. Privacy Notice	2
1.1. Policy Owner	2
1.2. Purpose and Scope.....	2
1.3. Responsibilities	2
1.4. Privacy Notice	3
1.4.1. Introduction & Scope	3
Controller contact details	3
1.4.2. The Personal information we process	3
1.4.3. How and why we use your Personal Data	4
Lawful bases for processing	5
1.4.4. Sharing your Personal Information	5
1.4.5. Data Retention	6
1.4.6. Protecting your Personal Data	6
Automated decision-making.....	7
1.4.7. Data Subject Rights	7
Publication and review	8
2. Version Control and Classification	9
1.0. Version	9
1.1. Classification	9

1. Privacy Notice

1.1. Policy Owner

The policy owner is the Board of Directors.

1.2. Purpose and Scope

This privacy notice explains how Cenit College collects, uses, stores, shares and protects personal data relating to its current and former employees, workers, contractors, temporary workers, volunteers and job applicants in Ireland and the United Kingdom. It supports compliance with applicable data protection legislation, including the EU General Data Protection Regulation (EU GDPR), the UK General Data Protection Regulation (UK GDPR), Ireland's Data Protection Acts 1988-2018, the UK Data Protection Act 2018 and relevant regulatory guidance.

1.3. 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.
Executive Board	Responsibility to execute the policy.
Head of Finance	Maintaining all financial records
Staff	Ensuring compliance in their respective roles and duties.
Director of Technology, Risk and Compliance	- 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
Head of Quality	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 GDPR and other data protection legislation. - 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, when requested by Cenit College. In performing their tasks, they consider the risk associated with processing operations and the nature, scope, context, and purposes of processing.
--	---

1.4. Privacy Notice

This notice is to be displayed on our website and all relevant external sites.

Cenit College Employee Privacy Notice: Ireland and the United Kingdom

1.4.1. Introduction & Scope

Cenit College is committed to data security and the lawful, fair, and transparent processing of personal data. This Privacy Notice describes how we process personal information about you in accordance with data protection regulations, including the EU General Data Protection Regulation (GDPR), Ireland's Data Protection Acts 1988-2018 and any relevant guidance issued by the Data Protection Commission (DPC), during and after your working relationship with us.

This notice applies to all current and former employees and volunteers, as well as candidates for new positions.

Cenit College adheres to the Data Protection Principles and will ensure that your personal data is:

- Processed lawfully, fairly and in a transparent manner.
- Collected for valid purposes, which are explained in this Privacy Notice, and not used in a way that is not compatible with these purposes.
- Adequate and relevant for these purposes
- Accurate and kept up to date.
- Kept only as long as necessary for these purposes and to meet any legal, statutory, or contractual obligation.
- Kept securely.

Cenit College is a 'controller' of your personal data. This means that we are responsible for deciding the purpose and means of processing your personal information.

Controller contact details

Cenit College, Unit 22 Tesco Monread Shopping Centre, Monread Road, Naas, Co. Kildare, Ireland, W91 YR12. For the purposes of applicable data protection legislation, Cenit College acts as the Data Controller for employee personal information. Data protection enquiries and rights requests may be sent to dataprotection@cenitcollege.ie.

1.4.2. The Personal information we process

We will collect, store, and use some or all of the following personal information. This may be collected directly from you or from various third parties, such as previous employers, recruitment agencies, and public sources, including social media channels (if you interact with us through those channels).

- Personal Contact details, including Name, title, address, telephone numbers, and email address.

- Details (and copies) of your communications and interactions with us, including by email, telephone and post.
- Copies or reference numbers of documents you provide as proof of identity. when you are initially employed or appointed by us, or where there is a legal reason to request these documents from you during the term of your employment/service.
- Information about your use of Cenit College information, systems, applications, and websites, including geolocation data.
- Dates of birth, marriage, and divorce
- Marital status and dependents
- Next of kin, emergency contact details, death benefit nominee(s)
- National Insurance Number/PPSN number.
- Bank account details.
- Payroll and tax information
- Salary, annual leave, pension, and benefits information (including insurance)
- Dates of employment/engagement
- We obtain and retain certificate numbers in relation to any criminal history or convictions as part of our background checks conducted at commencement, and when necessary, during your employment or service with us.
- Recruitment information (including copies of right to work documentation), personal and employer references and personal information provided in your CV. Interview notes and assessments (if applicable).
- Full employment/engagement records, which will include all or some of the following: contract, terms and conditions, job titles, work history, appraisals and performance information, absences (medical certificates/ information), training, and professional memberships.
- Health Information
- Grievance and Disciplinary information
- Details of any business or personal conflict of interest, at commencement and at regular intervals during your employment or service with us.
- Photographs (ID badge, intranet, publications)
- Accident-first aid records
- CCTV recordings (images may be captured at some locations)
- Telematics/GPS data
- When required, we will receive personal data from third-party organisations involved in Occupational Health assessments, or from your GP (with your explicit consent).
- Special category data (such as ethnicity, religious or philosophical beliefs) (which you may decide to share – optional)

Keeping your information up to date. Where your personal information is held in our HR, payroll self-service or Volunteer Management Provider (volunteers only) systems, it is your responsibility to ensure that the information (such as your address, contact details, bank account and next of kin) is kept up to date. If you're not sure how to do this, speak to your line manager/volunteer co-ordinator or HR for advice.

1.4.3. [How and why we use your Personal Data](#)

We will only use your personal information in accordance with the law. In most cases the processing of your Personal data (as listed in 2.0 Personal Information we process) is necessary to fulfil our obligations under your contract of employment or volunteer agreement, or to comply with legal, statutory, or contractual requirements.

Lawful bases for processing

Depending on the processing activity, Cenit College relies on one or more of the following lawful bases: taking steps before entering into and performing an employment or volunteer agreement; compliance with legal obligations; Cenit College's or a third party's legitimate interests, where those interests are not overridden by your rights and freedoms; protection of vital interests; and consent where appropriate. Where consent is used, it may be withdrawn at any time without affecting processing carried out before withdrawal.

Where we process special category data, we also identify an appropriate condition under Article 9 GDPR, including employment and social protection law, occupational health, legal claims, substantial public interest or explicit consent, as applicable. Criminal conviction and offence data is processed only where authorised by law and with appropriate safeguards.

This includes:

- To enable us to make a recruitment or appointment decision and to register you on to our Talent Pool (on request)
- Checking your eligibility to work for us.
- Administration of your employment contract/volunteering agreement
- To enable us to make payments to you and to deduct tax and social insurance contributions, including PRSI or National Insurance, where applicable.
- To administer pension funds, work benefits and insurance
- Appraisals and salary reviews
- Gathering evidence in relation to a possible grievance or disciplinary matter, including any legal disputes involving you or others.
- Managing sickness absence, including fitness to work
- Complying with Health and Safety obligations (including workplace adjustments)
- Education and training
- For equal employment opportunities (anonymised), monitoring and reporting.
- For network and information security purposes. (We may monitor your use of our systems to ensure compliance with our Information Security policies.

1.4.4. Sharing your Personal Information

We may share your personal data with all or some of the following trusted third parties:

- The Revenue Commissioners, HM Revenue and Customs (HMRC), the Department for Work and Pensions (DWP), and other statutory authorities where we are legally required to provide employee information for tax, social insurance, benefits or related purposes.
- Pension and Insurance providers as part of your contract of employment, and our legal obligations
- Stakeholders and commissioners where your role is in conjunction with a contract being delivered by one or more parts of the organisation.
- Cloud providers of software systems and solutions.
- External IT and Business Support Services used by the group in connection with the fulfilment of your contract of employment or your volunteer agreement,
- Professional advisers, including lawyers/Solicitors, medical professionals, bankers, auditors, and insurers, for the purposes of providing consultancy, legal, insurance and accounting services.

- An Garda Síochána, UK police services, safeguarding bodies and other regulatory or law-enforcement authorities as part of an investigation or for legal, safeguarding or regulatory purposes.
- Auditors, to audit our systems and processes for the purposes of ensuring efficiency, or regulatory or contractual compliance.
- UK and Irish law enforcement agencies and third-party security companies, for the purposes of ensuring that we comply with the law and have adequate security measures in place.
- Registered services, such as employee benefits providers, and authorised vetting services for Garda vetting or DBS checks where applicable (before and during employment or engagement).
- Approved External Training providers, to enable the registration process (name and business email address only).
- We will disclose your personal information to third parties if we are under a duty to disclose or share your personal data to comply with any other legal or regulatory obligation or request.
- With medical professionals, prospective employers and other third parties at your request and/or with your consent.

1.4.5. Data Retention

We will only keep your personal data for as long as necessary to fulfil the purposes for which we collected it, including to satisfy any legal or contractual requirements. Details of retention periods for different aspects of your personal information are provided in our Data Retention Schedule, which is available in our Information Management Policy.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

- Once you are no longer an employee or volunteer, we will retain and securely destroy your personal information in accordance with our data retention schedule or applicable laws and regulations. We may anonymise your personal information so that it can no longer be associated with you, in which case we will use such information without further notice to you.
- In some circumstances, you may be entitled to ask us to delete your data: see Data Subject Rights below for further information.

1.4.6. Protecting your Personal Data

- We have appropriate technical and organisational measures in place to prevent your personal data from being accidentally lost, used, altered, disclosed, or accessed in an unauthorised way.
- We apply role-based access controls, limiting access to your personal information to those employees and other third parties who have a business need to know.
- Our security controls are designed to maintain the confidentiality, integrity, and Availability of your personal information.
- We have procedures in place to deal with any data breach, or suspected breach, and will notify you and any applicable regulator where we are legally required to do so.
- Our group-wide staff training and awareness portfolio covers key risk areas and specific controls associated with your role.

- Wherever possible, we ensure the online cloud services are accessed using 'HTTPS' rather than 'HTTP', meaning that all information that is sent and received over the internet is encrypted for additional security. You can see this in your browser's address bar.
- We have selected and deployed technical measures such as password complexity requirements, anti-virus and anti-malware software, firewalls, encryption, email and internet filtering and VPNs for secure remote access.
- We have implemented soft controls such as our Information Security Policy, Data Protection Policy and Framework, Clear Desk and Clear Screen policies, the Individual User Agreement and Mobile Device policy.
- Where we disclose your personal data to third parties, we require the third party to have appropriate technical and organisational measures in place to protect your personal data, via robust contracts and agreements. In some instances, we may be compelled by law to disclose your personal data to a third party, and we have limited control over how that party protects it.
- Our systems and technical security controls are regularly audited by independent auditors to ensure we maintain our security accreditations.
- Some service providers may process personal data outside the European Economic Area (EEA) or the United Kingdom. Where this occurs, Cenit College will ensure that an applicable lawful transfer mechanism and appropriate safeguards are in place. These may include an adequacy decision or adequacy regulation, approve Standard Contractual Clauses, the UK International Data Transfer Agreement or UK Addendum, and supplementary measures where required.

Automated decision-making

Cenit College does not currently make employment, recruitment or engagement decisions based solely on automated processing, including profiling, where the decision would produce legal or similarly significant effects. If this changes, affected individuals will be informed, and the safeguards required by data protection law will be applied.

1.4.7. Data Subject Rights

You have the right:

- to ask us not to use your personal data for direct marketing.
- to ask us not to process your personal data where it is processed on the basis of legitimate interests, if there are no compelling reasons for that processing.
- to request from us access to personal information held about you (see below).
- to ask for the information we hold about you to be rectified if it is inaccurate or incomplete.
- to ask that we stop any consent-based processing of your personal data after you withdraw that consent.
- to ask, in certain circumstances, to delete the personal data we hold about you.
- to ask, in certain circumstances, for the processing of that information to be restricted.
- to ask, in certain circumstances, for data portability.

not to be subject to a decision based solely on automated processing, including profiling, where that decision produces legal or similarly significant effects, subject to the exceptions provided by law.

If you have any questions or concerns about this Privacy Notice, or require assistance with any data protection matter, please contact the Data Protection Manager by email to dataprotection@cenitcollege.ie

If you remain dissatisfied about how Cenit College processes your personal data, you have the right to lodge a complaint with the supervisory authority relevant to your location. Employees based in Ireland may complain to the Data Protection Commission (DPC). Employees based in the United Kingdom may complain to the Information Commissioner's Office (ICO).

- Data Protection Commission (Ireland): <https://www.dataprotection.ie/en>
- Information Commissioner's Office (United Kingdom): <https://ico.org.uk/>

Publication and review

This Employee Privacy Notice was last updated on the date below. It will be reviewed periodically and updated where there are material changes to Cenit College's processing activities, applicable data protection legislation or organisational arrangements. The current approved version will be published on the Cenit College website and made available to relevant employees, workers, contractors, temporary workers, volunteers and job applicants.

2. Version Control and Classification

1.0. Version

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	Date not recorded	Author not recorded	New Policy
2	23/10/2025	DPM	Minor Updates
3	24/08/2026	DTRC	Revised following comparison with the Seetec Employee Privacy Notice v4.1. Expanded the notice to cover employees, workers, contractors, temporary workers, volunteers and job applicants in Ireland and the United Kingdom. Added EU GDPR, UK GDPR and UK Data Protection Act 2018 references; jurisdiction-specific tax, social insurance, vetting and supervisory authority information; lawful bases; special-category and criminal-offence data conditions; international-transfer safeguards; automated decision-making information; and updated document title, scope, terminology and document-control information.

1.1. Classification

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

DOCUMENT CLASSIFICATION	Public
PRINTING	Uncontrolled when printed
DOCUMENT REF	QA8.9.1
VERSION	3
LAST APPROVAL DATE	24/08/2026