CENIT COLLEGE

Cenit College UK Data Protection Policy

033 0828 0953 enquiries@cenitcollege.co.uk www.cenitcollege.co.uk

Contents

1. Data Protection Policy 3
1.1 Introduction 3
1.2 Policy Owner 3
1.3 Purpose 3
1.4 Scope 4
1.5 Policy Statement 4
2. Responsibilities 4
3. Principles and Procedures 5
3.1 Data Protection Contact (Complaints and Enquiries) 5
3.2 Rights of the Data Subject 5
3.3 Consent for Data Processing 6
3.4 Third-Party Processors 7
3.5 Joint Data Controllers 7
3.6 Cenit College UK as a Processor 7
3.7 Data Collection Principles 8
3.8 Data Subject Rights Requests 11
3.9 Data Protection Impact Assessments (DPIA) 12
3.10 Special Categories of Personal Data 13
4. Monitoring and Review 13
5. References and Related Policies 14
5.1 References 14
5.2 Policies 14
6. Version Control 15
Appendix A: Summary of Key UK GDPR Provisions 16
i. Lawful Bases for Processing (Article 6 UK GDPR) 16
ii. Conditions for Consent (Article 7 UK GDPR) 16
iii. Special Categories of Personal Data (Article 9 UK GDPR) 16
iv. Data Subject Rights (Articles 12–23 UK GDPR) 16
v. Data Protection Impact Assessments (DPIAs) (Article 35 UK GDPR) 17

© 2026 Cenit College. All rights reserved. No part of this publication may be reproduced or shared in any form without prior written permission of the copyright owner, except where permitted by law. AI tools may have been used to develop some of the materials in this presentation.

1. Data Protection Policy

1.1 Introduction

Cenit College is committed to protecting the privacy, confidentiality, integrity, and security of personal data relating to learners, staff, contractors, partners, and other stakeholders. The College recognises its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable data protection and privacy legislation.

This Policy sets out the principles and requirements governing the collection, use, storage, disclosure, retention, and disposal of personal data by Cenit College. It establishes the responsibilities of all employees, contractors, and individuals acting on behalf of the College to ensure that personal data is processed lawfully, fairly, transparently, and securely.

Cenit College is committed to maintaining high standards of data protection and information governance, safeguarding the rights and freedoms of individuals, reducing the risk of data breaches, and fostering trust amongst learners, staff, partners, and other stakeholders through responsible and compliant data management practices.

1.2 Policy Owner

The policy owner is the Board of Directors.

1.3 Purpose

This policy aims to provide information and transparency regarding the Data Protection obligations of Cenit College UK to comply with all applicable Data Protection Regulations, including the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications (EC Directive) Regulations 2003. It applies to all processing of personal data undertaken by Cenit College UK relating to employees, learners, and other stakeholders. When processing personal data, Cenit College UK 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.

1.4 Scope

This policy applies to processing activities concerning personal and sensitive data carried out by Cenit College UK 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 UK. This cohort includes direct employees (full-time and part-time), tutors, etc.
- Third-party organisations that receive, handle or process personal data on behalf of Cenit College UK. This cohort is often referred to as a processor or sub-processor.

This Policy should be read in conjunction with: Privacy Notice - Cenit College

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 in accordance with EU and National legislation and is committed to implementing this 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 Cenit College staff member fail to process Personal Data in compliance with this policy, disciplinary proceedings may be initiated against them.

2. Responsibilities

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

Role	Responsibility
Board of Directors	Overall responsibility for Data Management within Cenit College UK.
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 Technology, Compliance and Risk	• Maintaining our server where data is held, i.e., security, configuration and maintenance.

Role	Responsibility
	• Back-up(s) • VLE and storage of data • Monitoring the IT environment and performing 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 UK activities.
Data Protection Manager (DPM)	We have appointed a Data Protection Manager who has the following responsibilities: • to inform and advise Cenit College UK and the employees who carry out processing of their obligations according UK data protection legislation, including UK GDPR. • Monitor compliance with the UK GDPR, other data protection legislation, and the policies of Cenit College UK 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 UK GDPR. • To cooperate with the Information Commissioner (IC). • To act as a contact point for the Information Commissioner (IC) 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 Information Commission (IC) 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.

3. Principles and Procedures

3.1 Data Protection Contact (Complaints and Enquiries)

All personal data enquiries or complaints should be made to Cenit College UK's DPM at the following email address: dataprotection@cenitcollege.co.uk

3.2 Rights of the Data Subject

Under UK GDPR, individuals have the following rights:

- to ask us not to use their personal data for direct marketing.

- to ask us not to process their personal data where it is processed based on legitimate interests if there are no compelling reasons for that processing.
- to request from us access to personal information held about them.
- to ask for the information we hold about them to be rectified if it is inaccurate or incomplete.
- to ask that we stop any consent-based processing of their personal data after they withdraw that consent.
- to ask, in certain circumstances, to delete the personal data we hold about them.
- to ask, in certain circumstances, for the processing of that information to be restricted; and
- to ask, in certain circumstances, for their data to be moved to another controller.

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

3.3 Consent for Data Processing

Under Article 7 of the UK GDPR legislation, where processing is based on consent, Cenit College UK will demonstrate that the data subject has consented to the processing of their personal data. Where consent is given by the data subject (for example, using personal data for marketing purposes), Cenit College UK obtains this consent in writing. Such consent will 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 UK will ensure that the following consent protocols are implemented.

- 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 pre-filled boxes will be displayed.
- Clear and plain language will 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 will be periodically reviewed to ensure currency and the legitimacy of purpose.

Refer to Appendix A for a breakdown of the conditions for valid consent under Article 7 UK GDPR.

3.4 Third-Party Processors

As a Controller, Cenit College UK may engage third parties to process Personal Data on its behalf. In such cases, a written contract will be established with the third party, clearly outlining their obligations regarding the processing of Personal Data, in compliance with UK GDPR practices. Cenit College UK will remain the 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 in accordance with UK GDPR requirements.

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

3.5 Joint Data Controllers

Cenit College UK may act as a Joint 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 UK GDPR, including transparency obligations and mechanisms for data subject rights.

In such cases, Cenit College UK 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 UK General Data Protection Regulation (UK GDPR).

Regardless of whether Cenit College UK is acting as a sole or joint controller, data subjects retain the right to exercise their UK GDPR rights directly with Cenit College UK. 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 in accordance with UK GDPR requirements. See Appendix A for lawful bases and responsibilities under joint controller arrangements, particularly Article 6 and Article 26 UK GDPR.

3.6 Cenit College UK as a Processor

In certain circumstances, Cenit College UK may act as a processor, processing personal data on behalf of another organisation (the 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 UK acts as a Processor, it does not determine the purpose or means of processing personal data but follows the Controller's documented instructions.

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

- **Processing personal data only on documented instructions** from the Controller, including regarding transfers to third countries or international organisations, unless required.
- **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 Controller** in fulfilling its obligations, particularly regarding:
    - Data Subject Access Requests (SARs)
    - Data Protection Impact Assessments (DPIAs)
    - Incident and breach notification
- **Not to engage any sub-processors without prior written authorisation of the Controller and to ensure** equivalent data protection obligations are imposed on any sub-processor.
- **Deleting or returning personal data** to the Controller upon completion of services, unless required by law to retain.
- **Maintaining a written record of processing activities** carried out on behalf of each Controller.

Where Cenit College UK is unsure of any instruction provided by the Controller or considers that an instruction may breach UK 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 in accordance with UK GDPR requirements.

3.7 Data Collection Principles

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

- Learners

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

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

Cenit College UK ensures that all data is:

1. *Processed lawfully, fairly and in a transparent manner in relation to the data subject.* Cenit College UK will always safeguard the rights and freedoms of the data subjects. Data processing will be carried out as follows.
    a. The data collected will be justified, i.e., legally or contractually necessary, etc., and collected as part of Cenit College UK's lawful activities.
    b. Where applicable, through 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 UK may share limited personal information relating to applicants and learners with Cenit College Head Office in Ireland (part of the Cenit group) for monitoring, statistical, and reporting purposes.
    f. Cenit College UK 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 is not considered to be incompatible with the initial purposes;* Cenit College UK will fulfil this obligation by:
    a. Only obtaining personal data for specific, lawful, and clearly stated purposes.
    b. Cenit College UK 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 UK holds their data.
3. *Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.* Cenit College UK 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 that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.* Cenit College UK will fulfil this obligation by.
    a. Ensuring that data accuracy and access are regularly assessed through defined mechanisms, such as 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 UK GDPR in order to safeguard the rights and freedoms of the data subject*. Cenit College UK 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 UK 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 UK will fulfil this obligation by.

a. Employing appropriate security standards to protect any personal data they hold. This includes measures to protect against unauthorised access, alteration, or destruction of such data.
b. Ensuring 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 UK 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 in completing 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 UK GDPR Articles 5 and 6, summarised in Appendix A.

3.8 Data Subject Rights Requests

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

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

Cenit College UK 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 UK, or believes that their rights as a data subject have not been addressed, they can make a formal complaint to the Information Commissioner's Office (ICO), which can be contacted as follows.

- Website: https://ico.org.uk
- Phone: 0303 123 1113
- Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

3.9 Data Protection Impact Assessments (DPIA)

Article 35 of the UK 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 UK will carry out a DPIA when the processing presents or could present a high risk to the rights and freedoms of the data subjects. UK 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. When the processing itself 'prevents data subjects from exercising a right or using a service or a contract'

Cenit Colleges' UK 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 UK GDPR, considering the rights and legitimate interests of data subjects and other persons concerned.

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

3.10 Special Categories of Personal Data

Under Article 9 of the UK GDPR, Cenit College UK 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 UK GDPR, refer to Appendix A.

4. Monitoring and Review

The **Director of IT** is responsible for monitoring the implementation and effectiveness of this Data Protection Policy in conjunction with the Board of Directors and the Data Protection Manager. This will include:

- Monitoring compliance with UK GDPR and Data Protection legislation.
- Reviewing data security incidents, breaches, and near misses.
- Conducting periodic audits of data processing activities and information security controls.
- Monitoring staff completion of mandatory data protection training.
- Reviewing requests relating to data subjects' rights and ensuring statutory deadlines are met.

- Reporting significant data protection risks, incidents, and compliance issues to the Senior Leadership Team.
- Ensuring the policy is reviewed at least annually or sooner where legislative or organisational changes require it.

5. References and Related Policies

5.1 References

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR) 2003
- Information Commissioner's Office (ICO) guidance and codes of practice
- Freedom of Information Act 2000 (if applicable)
- Human Rights Act 1998 (Article 8 - Right to Privacy)
- Equality Act 2010 (where processing involves special category data)

5.2 Policies

- Data Subject Access Request Procedure
- Data Breach Policy
- Data Breach Reporting Procedure
- Data Protection Training and Awareness Policy
- Information Security Policy
- Cyber Security Policy
- Data Breach Management Procedure
- Data Retention and Disposal Policy
- Subject Access Request Procedure
- Acceptable Use of ICT Policy
- Remote Working Policy
- Privacy Notice

6. Version Control

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	11/08/2025	KMCD, BF & JH	Check over and added a section on Cenit College UK as a processor. Word "Data" removed before Controller, Processor, Paragraph moved from Data Protection Contact to Data Subject Requests Reworded Rights of Data Subject so they are clearer now Other minor changes in wording.
6	07/11/2025	BF	Updated Information Commissioner's Office to Information Commission.
7	30/10/2026	HoQ & DTCR	Annual review. Transferred to the new Cenit template and renumbered all sections for policy standardisation. New sections added: 1.1 - Introduction, 4 - Monitoring and review, 5 - References and related policies. Updated Director of Technology, Compliance and Risk and Head of Quality titles.

Appendix A: Summary of Key UK GDPR Provisions

i. Lawful Bases for Processing (Article 6 UK 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 the performance of a contract.
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 Cenit's legitimate interests or those of a third party, unless overridden by the individual's rights.

ii. Conditions for Consent (Article 7 UK 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 UK GDPR)

These include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (when used for identification purposes)
- Health data
- Data concerning sex life or sexual orientation

Processing is prohibited unless one of the exemptions applies under Article 9:

- Explicit consent from the data subject
- Vital interests of the data subject or another person
- Legal obligations in the field of employment, social security, and social protection
- Legitimate activities by not-for-profit bodies
- Substantial public interest, such as preventing of detecting crime
- Public interest in areas such as public health
- Medical purposes and health care management
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for legal claims or whenever courts are acting in their judicial capacity

iv. Data Subject Rights (Articles 12–23 UK 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" (in certain circumstances)
- **Restrict processing** – under certain conditions
- **Data portability** – transfer data to another provider (in certain circumstances)
- **Object** – to processing based on legitimate interests, which always applies to direct marketing
- **Not be subject to automated decision-making** - including profiling

v. Data Protection Impact Assessments (DPIAs) (Article 35 UK 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 evaluate risks
- Identify Risk mitigation measures
- Document the outcome of the Assessment
- Keep under review

CENIT COLLEGE

Get in Touch

Telephone: 0330 82 0953
Email: enquiries@cenitcollege.co.uk
Website: www.cenitcollege.co.uk

Follow Us