GDPR & Data Protection Policy

Presented by: **Innovate Learning Centre CIC**

Author:	ASAD SARWAT
Approved by:	SMT
Date:	JAN 2026
Next Review Date:	JAN 2027

Registered Office: 73 Mellish Road, Walsall, England, WS4 2DG
Contact Address: 78a Walsall Road, Sutton Coldfield, Birmingham, B74 4QY
Phone: 0121 716 7286 | Email: info@innovatelearning.co.uk

1.0 Introduction

1.1 Purpose

This policy outlines Innovate Learning Centre CIC's commitment to protecting the personal data of staff, students, and partners. We uphold the principles of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.2 Scope

This policy applies to all data subjects whose personal information we hold, including applicants, current and former students, staff, and external stakeholders.

2.0 Principles of Data Protection

2.1 Lawfulness, Fairness and Transparency

All personal data is collected and processed lawfully, fairly, and in a transparent manner in relation to individuals.

2.2 Purpose Limitation

Data is collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

2.3 Data Minimisation

We ensure data collected is adequate, relevant and limited to what is necessary.

2.4 Accuracy

We take every reasonable step to ensure personal data is accurate and kept up to date.

2.5 Storage Limitation

Data is kept only for as long as necessary. Retention schedules are reviewed annually.

2.6 Integrity and Confidentiality

Data is processed securely, including protection against unauthorised or unlawful processing and against accidental loss or damage.

2.7 Accountability

Innovate Learning Centre CIC takes responsibility for compliance and has implemented appropriate technical and organisational measures.

3.0 Data Subject Rights

3.1 Right to Access

Individuals can request a copy of their personal data. Requests must be responded to within one month.

3.2 Right to Rectification

Data subjects may request corrections to inaccurate or incomplete data.

3.3 Right to Erasure

Also known as ‘the right to be forgotten’, this applies under specific conditions outlined in Article 17 of the UK GDPR.

3.4 Right to Restrict Processing

Individuals can request limited processing in certain circumstances.

3.5 Right to Data Portability

Where applicable, individuals can request data in a structured, commonly used and machine-readable format.

3.6 Right to Object

Individuals may object to processing based on legitimate interest, public task, or direct marketing.

4.0 Data Collection and Use

4.1 Learner Data

We collect student data for purposes of enrolment, funding (e.g. ESFA), learning delivery, assessment, safeguarding, and progression.

4.2 Staff Data

Used for employment, payroll, training, appraisals and internal operations.

4.3 Visitors and Stakeholders

Names, contact details, and interaction logs are recorded for legitimate business use.

4.4 Consent

Where required, consent is sought explicitly and can be withdrawn at any time.

5.0 Data Storage and Security

5.1 IT Systems

All personal data is stored securely with password protection, encryption and access logs.

5.2 Paper Records

Locked in cabinets in restricted areas, only accessible by authorised staff.

5.3 Remote Access

Staff accessing data remotely must use secure VPN and encrypted devices.

5.4 Breach Notification

All suspected data breaches must be reported immediately to the Data Protection Officer (DPO). Serious breaches will be reported to the ICO within 72 hours.

6.0 Responsibilities

6.1 Data Protection Officer (DPO)

Oversees compliance, delivers training, handles subject access requests, and responds to data breaches.

6.2 All Staff

Must complete annual GDPR training, follow safe practices, and report concerns promptly.

6.3 SMT

Ensure policies and procedures are embedded across departments.

7.0 Third Party Processors

7.1 Contracts

Where personal data is shared with third parties (e.g. cloud storage, software providers), Data Processing Agreements are in place.

7.2 Due Diligence

Vendors are assessed for GDPR compliance prior to engagement.

8.0 Data Retention and Disposal

8.1 Retention Schedules

Retention periods are based on legal, regulatory and funding requirements.

8.2 Secure Disposal

Data is destroyed securely when no longer needed – shredded, deleted from systems, or wiped electronically.

9.0 Monitoring and Review

9.1 Annual Review

The policy is reviewed annually and updated to reflect legal, regulatory and organisational changes.

9.2 Audits

Internal audits assess policy implementation and identify areas for improvement.