1.7 Data Protection Policy

Version Control

Version	Date	Description	Author
1.0	January 2024	Initial Policy Development	C-TAC
2.0	November 2024	Updated to include TAQA system integration	C-TAC

1.7.1 Purpose

This policy outlines C-TAC's commitment to safeguarding the confidentiality, integrity, and availability of personal data in compliance with GDPR, PHECC standards, and TAQA quality assurance principles.

1.7.2 Scope

This policy applies to all C-TAC staff, faculty, learners, and external stakeholders who handle personal data during training, assessment, and administrative processes.

1.7.3 Data Protection Principles

- **Lawfulness, Fairness, and Transparency:** Personal data is processed lawfully, fairly, and transparently.
- **Purpose Limitation:** Data is collected for specific, legitimate purposes.
- **Data Minimisation:** Only the data necessary for the intended purpose is collected.
- **Accuracy:** Personal data is kept accurate and up-to-date.
- **Storage Limitation:** Data is retained only as long as necessary.
- **Integrity and Confidentiality:** Data is processed securely to prevent unauthorised access, disclosure, or loss.

1.7.4 Process

1. **Data Collection:**
    - Personal data is collected through registration forms, assessments, and feedback surveys.
    - Learners are informed about the purpose of data collection and their rights under GDPR.
2. **Data Storage:**
    - Digital data is stored securely on C-TAC's internal systems with encrypted access.
    - Physical documents are stored in locked cabinets with limited access.

3. **Data Access:**
    - Access to personal data is restricted to authorised personnel based on their roles.
    - Affiliate faculty must sign confidentiality agreements before accessing learner data.
4. **Data Sharing:**
    - Personal data is shared only with approved third parties for external verification, in accordance with GDPR.
    - Data is not disclosed to unauthorised individuals or organisations.
5. **Data Retention:**
    - Personal data is retained for three years after the learner's completion of training unless required for regulatory purposes.
    - After the retention period, data is securely deleted or shredded.
6. **Data Breach Management:**
    - Any suspected or actual data breaches must be reported to the Data Protection Officer (DPO) within 24 hours.
    - The DPO investigates breaches, implements corrective actions, and reports incidents to the Data Protection Commission if necessary.
7. **Learner Rights:**
    - Learners can request access to their personal data, request corrections, or request data deletion.
    - Requests are processed within 30 days, and records of requests are maintained.

1.7.5 Responsibilities

- **Board of Directors:** Provides oversight of data protection compliance.
- **Director of Training:** Ensures that all data processing aligns with GDPR and PHECC standards.
- **Data Protection Officer (DPO):** Manages data protection processes, investigates breaches, and ensures compliance.
- **All Staff and Faculty:** Responsible for handling personal data securely and reporting any data protection concerns.

1.7.6 Monitoring and Review

- Data protection practices are reviewed annually to ensure compliance with GDPR and regulatory requirements.
- Internal audits verify that personal data is collected, stored, and processed securely.
- Feedback from stakeholders is used to improve data protection measures.

1.7.7 Approval and Compliance Monitoring

- **Approved by:** Adrian Coffey, Director of Training
- **Date:** October 2024
- Compliance with this policy is monitored through regular audits and verification.