Data Protection Policy

This policy explains how the organisation collects, uses, stores, shares, and protects personal data relating to:

- apprentices
- staff
- employers
- visitors
- other stakeholders

It ensures compliance with UK GDPR, the Data Protection Act 2018, and DfE funding rules.

This policy applies to:

- all employees
- contractors
- workplacement/employer partners who access learner information
- volunteers
- anyone handling data on behalf of the provider

It covers all data processed in any format (electronic, paper, email, cloud, recordings, etc.).

Principles of Data Protection

We commit to processing data lawfully, fairly, and transparently. All personal data will be:

1. Used lawfully and fairly
2. Collected for specific, explicit purposes (e.g., funding, education, safeguarding)
3. Limited to what is necessary
4. Accurate and kept updated
5. Stored securely and retained only as long as needed
6. Processed with integrity and confidentiality

Lawful Bases for Processing

We process data under one or more of the following:

- **Contract** (managing apprenticeships, employer agreements)
- **Legal obligation** (DfE funding requirements, safeguarding duties)
- **Public task** (education and training)
- **Legitimate interests** (quality assurance, service improvement)

- **Consent** (photography, marketing, optional services)
- **Vital interests** (protecting life, safeguarding emergencies)

Types of Data We Collect

Apprentices

- Contact details
- Date of birth, gender
- Learning records (ILR, progress reviews, assessments)
- Employment details
- Attendance and engagement data
- SEND or medical needs (where relevant)
- Safeguarding information (when necessary)

Employers

- Contact and contract information
- Workplace details
- Mandatory compliance information

Staff

- HR records
- Training and CPD information
- Payroll and contractual details

We use personal data for:

- Enrolling apprentices and delivering training
- Funding claims and audit requirements
- Quality assurance and performance monitoring
- Safeguarding and wellbeing support
- Communication with learners and employers
- Compliance with ESFA, Ofsted, and legal duties

We will never sell personal data.

Data may be shared with:

- DfE
- Awarding organisations
- Ofsted
- Employers (where it relates to apprenticeship delivery)

- Safeguarding partners (police, local authorities, NHS)
- IT system providers (MIS, e-portfolio systems)

Sharing is strictly limited to what is necessary, secure, and lawful.

We ensure appropriate technical and organisational measures including:

- Password protection
- Secure MIS and e-portfolios
- Encrypted devices
- Restricted access based on role
- Secure disposal of records
- Staff training in data protection and cyber safety

Paper records are stored in locked cabinets and digital data is stored on secure servers or approved platforms.

Retention follows:

- DfE funding guidance
- Ofsted requirements
- Statutory duties (e.g., safeguarding records)
- Internal retention schedule

Apprenticeship records are typically retained for 6 years after completion unless regulations require longer.

Individuals have rights to:

- access their data
- request correction
- request deletion (where legally possible)
- restrict processing
- object to certain uses
- data portability

All staff must report suspected breaches immediately.
The organisation will:

- investigate promptly
- record the incident
- notify Caretech team
- inform affected individuals when required

Responsibilities

All staff

- Follow this policy
- Keep data secure
- Report concerns or breaches

Managers

- Monitor compliance
- Ensure staff training
- Maintain safe systems

Data Protection Officer (DPO)

- Oversee compliance
- Respond to data subject requests
- Report serious breaches

Training

All staff receive mandatory annual training on:

- data protection
- cyber security
- secure data handling
- GDPR awareness

Additional training is provided for managers and anyone handling sensitive or safeguarding information.