



The Link Training Academy

Data Protection and Information Governance Policy

Version: V1 2026-2027

Policy Owner: Director / Data Protection Lead

Approved By: Directors

Review Date: August 2027

1. Policy Statement

The Link Training Academy is committed to protecting the privacy, confidentiality, integrity and security of personal information.

We recognise our responsibilities under:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Freedom of Information legislation where applicable;
- Safeguarding legislation and statutory guidance;
- Information Commissioner's Office (ICO) requirements.

The Link Training Academy processes personal information relating to learners, apprentices, employers, staff, contractors and other stakeholders. We are committed to ensuring that personal information is processed lawfully, fairly, transparently and securely.

This policy supports The Link Training Academy's commitment to safeguarding learners, maintaining public confidence and meeting regulatory requirements.

2. Purpose

The purpose of this policy is to:

- Protect the rights of individuals whose data we process.
 - Ensure compliance with UK data protection legislation.
 - Establish clear responsibilities for handling information.
 - Promote effective information governance.
 - Support safeguarding and learner welfare obligations.
 - Minimise the risk of data breaches and cyber incidents.
 - Provide guidance on data sharing, retention and disposal.
-

3. Scope

This policy applies to:

- All employees;
- Associates and consultants;
- Volunteers;
- Contractors;
- Directors;
- Apprentices;
- Learners;
- Employers and workplace mentors where relevant;
- Any individual processing personal data on behalf of The Link Training Academy.

The policy applies to information held:

- Electronically;
 - In paper records;
 - Within cloud systems;
 - Through email and messaging systems;
 - Within learning management systems;
 - During remote working activities.
-

4. Definitions

Personal Data

Any information relating to an identifiable living individual.

Examples include:

- Name;
- Address;

- Date of birth;
- Email address;
- Telephone number;
- National Insurance number;
- Learner reference numbers;
- Employment details.

Special Category Data

Information requiring additional protection, including:

- Health information;
- Disability information;
- Ethnicity;
- Religious beliefs;
- Trade union membership;
- Biometric data where applicable.

Criminal Offence Data

Information relating to:

- Criminal proceedings;
- Convictions;
- Cautions;
- DBS information.

5. Data Protection Principles

The Link Training Academy will ensure personal data is:

Lawful, Fair and Transparent

Individuals will be informed about how and why their data is processed.

Collected for Specified Purposes

Information will only be used for lawful and legitimate purposes.

Adequate, Relevant and Limited

Only information necessary for the stated purpose will be collected.

Accurate and Kept Up to Date

Reasonable steps will be taken to maintain accurate records.

Retained Only as Long as Necessary

Information will not be retained longer than required.

Secure

Appropriate technical and organisational measures will protect personal information.

Accountable

The Link Training Academy will be able to demonstrate compliance with UK GDPR requirements.

6. Roles and Responsibilities

Directors

Directors have overall responsibility for ensuring compliance with data protection legislation.

Responsibilities include:

- Approving policies;
- Monitoring organisational compliance;
- Responding to significant information governance risks.

Data Protection Lead

The Data Protection Lead will:

- Provide advice on compliance;
- Monitor implementation of this policy;
- Investigate data breaches;
- Coordinate responses to Subject Access Requests;
- Liaise with the Information Commissioner's Office where necessary.

Managers

Managers must:

- Ensure staff understand their responsibilities;
- Implement secure working practices;
- Report incidents promptly.

All Staff

All staff are responsible for:

- Protecting personal data;
 - Following organisational procedures;
 - Keeping information secure;
 - Reporting breaches immediately;
 - Completing mandatory training.
-

7. Lawful Basis for Processing

The Link Training Academy processes personal data under one or more lawful bases, including:

Legal Obligation

For example:

- Funding requirements;
- Apprenticeship compliance;
- Safeguarding duties;
- Employment law obligations.

Contract

Where processing is necessary to deliver training or employment arrangements.

Legitimate Interests

Where processing is necessary for the legitimate operation of the organisation.

Vital Interests

Where information must be processed to protect someone's life or safety.

Consent

Where consent is required, individuals will be informed:

- Why information is needed;
- How it will be used;
- Their right to withdraw consent where applicable.

The Link Training Academy recognises that consent is not the primary lawful basis for most learner and apprenticeship data processing.

8. Information We May Process

Information may include:

Learners and Apprentices

- Contact information;
- Eligibility evidence;
- Funding evidence;
- Attendance and progress data;
- Assessment records;
- Achievement records;
- Additional learning support information;
- Safeguarding records.

Staff

- Recruitment records;
- Payroll information;
- Performance information;
- Training records;
- DBS information where applicable.

Employers

- Contact information;
 - Workplace learning arrangements;
 - Apprenticeship documentation.
-

9. Safeguarding and Information Sharing

The Link Training Academy recognises that effective safeguarding sometimes requires the sharing of information.

Personal information may be shared without consent where there is a lawful basis to do so, including where:

- A child is at risk of harm;
- An adult at risk requires protection;
- A crime may have occurred;
- There is a safeguarding concern;
- A Prevent concern has been identified.

Information sharing decisions will be:

- Necessary;
- Proportionate;
- Relevant;
- Recorded appropriately.

Safeguarding considerations will take precedence where an individual may be at risk of harm.

Safeguarding records will be maintained and retained in accordance with the Safeguarding Policy and approved retention schedule.

10. Under-18 Learners

The majority of learners supported by The Link Training Academy are adults.

Where learners are under 18 years of age:

- Additional safeguarding considerations apply;
- Information will be processed in accordance with safeguarding requirements;
- Parents or carers may be involved where appropriate and lawful;
- Information sharing decisions will prioritise learner welfare and safety.

11. Security of Information

The Link Training Academy uses appropriate administrative, technical and physical safeguards to protect personal data.

Measures include:

- Password-protected systems;
- Multi-factor authentication;
- Access controls;
- Secure cloud-based storage;
- Encrypted devices where appropriate;
- Secure disposal arrangements;
- Staff training;
- Cyber security awareness.

Access to personal information is restricted to those who require it for legitimate business purposes.

12. Remote Working and Homeworking

As The Link Training Academy operates primarily through remote and workplace-based delivery, all staff must ensure that:

- Devices are protected by passwords;
- Screens are locked when unattended;
- Personal information is not accessible to unauthorised individuals;
- Documents are stored securely;
- Information is not downloaded unnecessarily;
- Data is only accessed through approved systems.

Learner information must not be stored on unauthorised devices or shared through personal email accounts.

13. Data Sharing

The Link Training Academy may share information with:

- Department for Education (DfE);
- Department for Work and Pensions (DWP)
- Awarding Organisations;
- End Point Assessment Organisations;
- Employers where appropriate;
- Regulatory inspection bodies;
- Safeguarding agencies;
- Law enforcement agencies;
- Professional advisers.

Data sharing will only take place where there is:

- A lawful basis;
- A contractual requirement;
- A safeguarding need;
- A legal obligation.

Appropriate data sharing agreements will be in place where required.

13A. Artificial Intelligence and Automated Technologies

The Link Training Academy may utilise approved technologies to support learning, assessment, quality assurance and information governance activities.

This may include:

- Plagiarism detection systems
- Authorship verification tools

- Artificial intelligence detection tools
- Learning Management Systems
- Learning technologies
- Quality assurance systems
- Cybersecurity and monitoring tools
- Approved suppliers and service providers acting on behalf of The Link Training Academy

Where artificial intelligence technologies are used, they will be applied in accordance with:

- UK GDPR
- Data Protection Act 2018
- Awarding Organisation requirements
- Information Technology, Cyber Security, Online Safety and Acceptable Use Policy
- Malpractice, Maladministration, Academic Integrity and AI misuse Policy.

The organisation does not make decisions that have legal or significant effects on individuals based solely on automated processing.

Appropriate human oversight and professional judgement will always be applied.

Individuals' rights relating to automated decision-making and profiling will be respected in accordance with UK GDPR requirements.

14. Subject Access Requests (SARs)

Individuals have the right to request a copy of personal information held about them.

Requests should be submitted to:

The Data Protection Lead – Benjamin Lodge – Ben@thelinktraining.org
The Link Training Academy

The organisation will normally respond within:

One calendar month

Where requests are particularly complex, an extension may be applied in accordance with UK GDPR.

15. Individual Rights

Individuals have the right to:

- Be informed;
- Access their personal data;
- Request correction of inaccurate data;
- Request erasure where appropriate;
- Restrict processing in certain circumstances;

- Object to processing in certain circumstances;
- Data portability where applicable;
- Protection from solely automated decision-making where applicable.

Requests will be considered in accordance with UK GDPR requirements.

16. Data Breaches

A data breach may include:

- Loss of information;
- Unauthorised disclosure;
- Unauthorised access;
- Cyber attack;
- Accidental deletion;
- Misdirected emails.

All suspected breaches must be reported immediately to the Data Protection Lead.

The organisation will:

1. Assess the incident.
2. Contain the breach where possible.
3. Investigate the circumstances.
4. Record the incident.
5. Implement corrective actions.
6. Notify affected individuals where required.
7. Notify the Information Commissioner's Office within 72 hours where legally required.

A central breach log will be maintained.

17. Retention and Disposal

Data retention periods are detailed within the organisation's Data Retention Schedule and are determined by legal, funding, safeguarding, employment and Awarding Organisation requirements.

- Learner records;
- Apprenticeship records;
- Funding documentation;
- Safeguarding records;
- Complaints records;
- Personnel records;

- Financial records;
- DBS information.

Information will be:

- Securely archived where required;
 - Securely deleted when no longer needed;
 - Destroyed confidentially where held in paper format.
-

18. Marketing, Photography and Publicity

The Link Training Academy may use photographs, videos, testimonials and learner success stories for promotional purposes.

Appropriate permissions will be obtained where required.

Individuals may withdraw consent for promotional use where consent is the lawful basis being relied upon.

19. CCTV

Where CCTV is operated within premises controlled by The Link Training Academy, separate CCTV procedures will apply.

Use of CCTV will be:

- Lawful;
 - Necessary;
 - Proportionate;
 - Clearly signposted.
-

20. Training and Awareness

All staff will receive:

- Data protection induction;
- Annual refresher training;
- Cyber security awareness training;
- Additional training where required by their role.

Compliance with data protection requirements forms part of every staff member's responsibilities.

21. Complaints

Individuals who are dissatisfied with how The Link Training Academy has handled their personal information should initially contact the Data Protection Lead.

Complaints may also be made through The Link Training Academy Complaints Policy.

Individuals have the right to contact the Information Commissioner's Office (ICO) if concerns remain unresolved.

22. Monitoring and Review

The Link Training Academy will monitor compliance through:

- Internal reviews;
- Policy audits;
- Breach monitoring;
- Safeguarding reviews;
- Quality assurance activities.

This policy will be reviewed annually, or sooner where:

- Legislation changes;
- Regulatory requirements change;
- Significant incidents occur;
- Organisational needs change.

Related Policies

- Safeguarding Policy – including Adults at Risk
- Bullying, Harassment and Respectful Behaviour Policy
- Information Technology, Cyber Security, Online Safety and Acceptable Use Policy
- Complaints Policy and Procedure
- Data Retention Schedule
- Staff Code of Conduct
- Information Security Policy
- Whistleblowing, Fraud Prevention and Anti-Bribery Policy
- Privacy Notice

Policy Owner: Directors

Responsible Lead: Data Protection Lead

Approved By: Board of Directors

Review Date: August 2027