Form Title: Data Protection
Form Ref: POL 012
Author: PRB Consulting
Date: May 2026
Version: V1.0

DATA PROTECTION POLICY

POLICY STATEMENT

The Company is committed to protecting the privacy, confidentiality, integrity and security of personal data and ensuring compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and all applicable data protection legislation.

The Company recognises that personal data is a valuable asset and will ensure that all personal data is processed lawfully, fairly, transparently and securely.

This policy outlines how personal data is collected, used, stored, shared and protected and applies to all individuals whose personal data is processed by the Company.

SCOPE

This policy applies to all personal data processed by the Company relating to:

- Employees and workers
- Learners, apprentices and trainees
- Prospective learners and applicants
- Job applicants
- Contractors and agency workers
- Clients and customers
- Suppliers and service providers
- Visitors to Company premises
- Business partners
- Any other individual whose personal data is processed by the Company

This policy applies to all employees, contractors, consultants and individuals acting on behalf of the Company.

DATA PROTECTION RESPONSIBILITY

The Company has appointed a Data Protection Lead who is responsible for overseeing compliance with data protection legislation and this policy.

Data Protection Lead / Responsible Person
Name: [Insert Name]
Position: [Insert Position]
Email: [Insert Email Address]
Telephone: [Insert Telephone Number]

Where required by law, the Company will appoint a Data Protection Officer (DPO).
The Data Protection Lead is responsible for:

- Monitoring compliance with data protection legislation.
- Advising management on data protection obligations.
- Managing data protection risks.
- Coordinating responses to data subject requests.
- Managing data breach reporting procedures.
- Acting as the primary point of contact for data protection enquiries.

© PRB Consulting Controlled & Published Document 2026

DATA PROTECTION PRINCIPLES

The Company will comply with the UK GDPR principles by ensuring personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Retained only for as long as necessary.
- Processed securely and protected against unauthorised access, loss, destruction or damage.
- Processed in a manner that demonstrates accountability and compliance.

DEFINITIONS

Personal Data

Any information relating to an identified or identifiable living individual.

Special Category Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, sex life or sexual orientation.

Processing

Any operation performed on personal data including collection, recording, storage, retrieval, use, disclosure, sharing, amendment, deletion or destruction.

LAWFUL BASIS FOR PROCESSING

The Company will only process personal data where there is a lawful basis for doing so, including:

- Consent.
- Performance of a contract.
- Compliance with a legal obligation.
- Protection of vital interests.
- Performance of a task carried out in the public interest.
- Legitimate business interests.

Special category data will only be processed where an additional lawful condition applies under the UK GDPR and Data Protection Act 2018.

HOW PERSONAL DATA MAY BE USED

The Company may process personal data for purposes including:

- Recruitment and selection.
- Employment administration.
- Learner enrolment and programme delivery.
- Assessment, monitoring and achievement recording.
- Safeguarding and welfare support.
- Customer relationship management.
- Contract management.
- Regulatory and funding compliance.
- Health and safety management.
- Equality, diversity and inclusion monitoring.
- Financial administration and payments.
- Legal and regulatory obligations.
- Business management and operational purposes.

© PRB Consulting Controlled & Published Document 2026

Personal data will only be used for legitimate purposes and will not be processed in a manner incompatible with those purposes.

DATA SECURITY

The Company will implement appropriate technical and organisational measures to protect personal data, including:

- Access controls.
- Password protection.
- Encryption where appropriate.
- Secure storage systems.
- Anti-malware protection.
- Firewalls and network security controls.
- Regular security reviews and audits.
- Staff training and awareness programmes.
- Secure disposal of records.

Access to personal data will be restricted to authorised individuals who require access for legitimate business purposes.

DATA RETENTION

Personal data will only be retained for as long as necessary to fulfil the purposes for which it was collected and to meet legal, regulatory or contractual requirements.
Records will be securely deleted, destroyed or anonymised when no longer required.
Retention periods will be defined within the Company's Records Retention Schedule.

SHARING PERSONAL DATA

The Company may share personal data where necessary with:

- Regulatory authorities.
- Awarding organisations.
- Funding bodies.
- Professional advisers.
- Service providers acting on the Company's behalf.
- Government departments and agencies.
- Law enforcement agencies where legally required.

Appropriate safeguards and contractual controls will be implemented where personal data is shared with third parties.

INDIVIDUAL RIGHTS

Individuals have the right to:

- Be informed about how their data is used.
- Access their personal data.
- Request correction of inaccurate information.
- Request erasure of personal data where appropriate.
- Restrict processing.
- Object to processing.
- Request data portability where applicable.

© PRB Consulting Controlled & Published Document 2026

• Withdraw consent where processing is based on consent.
• Challenge decisions made solely by automated processing.

Requests relating to these rights should be submitted to the Data Protection Lead.

SUBJECT ACCESS REQUESTS
Any individual may request access to personal data held about them.
Requests should be submitted in writing to the Data Protection Lead.
The Company will normally respond within one calendar month of receiving a valid request unless an extension is permitted under applicable legislation.

DATA BREACHES
A personal data breach includes any accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to, personal data.
All actual or suspected breaches must be reported immediately to the Data Protection Lead.
The Company will investigate all reported breaches and, where required, notify:

• The Information Commissioner's Office (ICO) within 72 hours.
• Affected individuals where there is a high risk to their rights and freedoms.

TRAINING AND AWARENESS
All employees and individuals handling personal data on behalf of the Company will receive appropriate data protection training.

Training will include:
• UK GDPR requirements.
• Data Protection Act 2018 obligations.
• Data security responsibilities.
• Recognising and reporting data breaches.
• Data subject rights.
• Information security good practice.

NON-COMPLIANCE
Failure to comply with this policy may result in disciplinary action and, where appropriate, legal action.
Contractors, suppliers or third parties who breach this policy may have their contracts terminated.

POLICY REVIEW
This policy will be reviewed annually or sooner where there are significant legislative, regulatory or organisational changes.

Signed: 

Name: R. Richardson

Role: Managing Director

Date: May 2026

© PRB Consulting Controlled & Published Document 2026