Karen Blake Coaching Ltd

DATA PROTECTION POLICY AND PROCEDURE

Karen Blake Coaching Ltd – Data Protection Policy

1. Policy Statement

Karen Blake Coaching Ltd ("KBC") is committed to full compliance with data protection legislation, specifically the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. KBC recognises the importance of safeguarding personal data relating to learners, clients, partners, contractors, suppliers, staff, and other individuals.

This policy sets out how personal data is collected, used, stored, shared, and protected by KBC.

2. Scope

This policy applies to:

- All employees, freelance trainers, assessors, IQAs, and contractors working for KBC.
- All locations, systems, and processes where personal data is processed.
- All personal data processed by KBC in connection with its coaching, training, assessment, consultancy, and business services.

3. Responsibilities

- The Director of KBC has overall responsibility for ensuring compliance with data protection legislation.
- All staff and contractors must comply with this policy and attend relevant training as required.
- Data protection enquiries, subject access requests, and data breaches should be reported to:
  Data Controller: Karen Blake (Director)
  Email: karen@karenblakecoaching.com

4. Principles of Data Protection

KBC processes personal data in accordance with the UK GDPR principles, ensuring that 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 to protect against unauthorised access, loss, or damage.

5. Types of Personal Data Processed

KBC may collect and process the following data:

- Names, addresses, contact details.
- Employment or educational information (where relevant to training/assessment).
- Assessment records and certification data.
- Financial and invoicing details (business clients only).
- Communication records (e.g. emails, enrolment forms, support requests).

KBC does not process sensitive special category data unless strictly necessary for training or funding purposes.

6. Data Storage & Security

- All electronic data is securely stored on password-protected systems and servers, with appropriate firewall and anti-virus protection.
- Data backups are taken regularly and securely stored.
- Paper records are securely stored in locked cabinets when not in use and shredded when no longer required.
- Data is only accessed by authorised personnel.
- No personal data is stored on unsecured personal devices.

7. Data Sharing

- Personal data may be shared with awarding bodies, regulatory authorities, funding bodies, or government agencies where required by law or contractual obligation.
- Data may also be shared with professional subcontractors involved in course delivery (tutors, assessors, IQAs), under strict confidentiality agreements.
- KBC does not sell or transfer personal data for marketing purposes.

8. International Transfers

- KBC does not routinely transfer personal data outside the UK.
- Any international transfers will comply with UK data protection laws and adequate safeguards.

9. Individual Rights

Under the UK GDPR, individuals have the following rights:

- Right to be informed.
- Right of access (subject access request).
- Right to rectification.
- Right to erasure (where applicable).
- Right to restrict processing.
- Right to data portability.
- Right to object.
- Rights related to automated decision making (which KBC does not use).

Subject access requests should be made to the Data Controller. KBC will respond within one calendar month.

10. Data Retention

KBC retains personal data only for as long as necessary for contractual, legal, or regulatory reasons. Retention periods are set according to:

- Awarding body requirements.
- Contractual or funding requirements.
- Legal obligations (e.g. tax, accounting).

Data is securely deleted or destroyed when no longer required.

11. Data Breaches

Any data breach will be reported to the Director immediately. Where legally required, KBC will notify the Information Commissioner's Office (ICO) within 72 hours.

12. Training & Awareness

All KBC staff, contractors, assessors, and partners receive appropriate training on data protection requirements and are expected to comply fully with this policy.

13. Related Policies

This policy should be read alongside:

- Confidentiality Policy (QAD 005)
- Safeguarding Policy
- IT Security Policy
- Whistleblowing Policy

14. Review
This policy is reviewed annually, or earlier if legislative changes occur.

Signed:
Karen Blake
Director
Date: June 2025