Carver Coaching
www.carvercoaching.co.uk

INFORMATION SECURITY POLICY 2025

1. Purpose

This policy sets out the information security controls used by Carver Coaching Ltd ("CC") to protect personal data and confidential information processed during the delivery of coaching, leadership development, facilitation and organisational development services.

This policy supports compliance with:

- UK GDPR
- Data Protection Act 2018
- Client confidentiality requirements
- NHS information governance expectations

2. Scope

This policy applies to:

- All Carver Coaching Ltd directors, associates and contractors
- All devices used for delivering services (laptops, phones, tablets)
- All personal data processed in connection with coaching or OD work

3. Security Roles and Responsibilities

- The Director of CC is responsible for overseeing information security and data protection practices.
- All associates must follow this policy and promptly report any security concerns or breaches.

4. Technical Security Measures

Carver Coaching Ltd implements the following controls:

4.1 Device Encryption

- All laptops use full-disk encryption
- All iPhones/iPads/Smartphones used for business purposes use built-in hardware encryption with passcodes enabled.

4.2 Multi-Factor Authentication (MFA)

- MFA is enabled on all accounts containing client data (Microsoft 365, OneDrive, SharePoint, email accounts).

4.3 Secure Storage

- Digital files are stored in secure, access-controlled cloud environments (Microsoft OneDrive or SharePoint).
- Coaching notes are pseudonymised and stored separately from identifiable information.

4.4 Anti-Malware & Updates

- All devices have up-to-date antivirus and firewall protection.
- Operating systems and applications are updated regularly.

4.5 Secure Communications

- Email is the primary communication channel; sensitive documents are password-protected if required.
- Public Wi-Fi is not used to access client data unless via VPN.
- No client personal data is shared via consumer messaging apps (e.g., WhatsApp).

5. Organisational Security Measures

5.1 Access Control

- Only the assigned coach may access coaching notes or related data.
- Associates receive only the information necessary for their assignment.

5.2 Pseudonymisation of Coaching Notes

- Coachee identities (name, role) are stored separately from coaching notes.
- Notes are labelled with unique ID codes rather than names.

5.3 Data Minimisation

- Only data strictly necessary for coaching or OD delivery is collected.
- Sensitive personal data is processed only when volunteered by the coachee's objectives.

5.4 Retention & Disposal

- Coaching notes retained for 6 months after programme completion, then securely deleted or shredded.
- Evaluation data may be anonymised and retained for service improvement.

5.5 Breach Management

- Any suspected or actual data breach is reported immediately to the Director.
- The Director will investigate and notify affected clients where required under UK GDPR.

6. Associate and Contractor Requirements

All associates must:

- Sign confidentiality and data protection agreements
- Store all client data according to this policy
- Use encrypted devices with MFA enabled
- Maintain up-to-date awareness of GDPR and confidentiality requirements relevant to their role.

7. Review

This policy is reviewed annually or following significant organisational or legislative change.

Signed: 

Name: LISA MARTIN, MANAGING DIRECTOR OF CARVER COACHING LTD
Dated: January 10th, 2025