Cyber Security & Data Protection Policy
Evolution Management Consultancy Ltd

Evolution Management Consultancy Ltd ("EMC") is committed to protecting the confidentiality, integrity, and availability of all data it holds—particularly sensitive information relating to fire safety, coatings compliance, and client site assessments. We operate in full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy outlines how we manage cyber security risks and protect personal and project-related data in our capacity as a specialist coatings consultancy.

This policy applies to:

- All EMC employees, subcontractors, and consultants
- All systems used to store or process data (e.g. email, file storage, CRM systems)
- All personal data collected in the course of business, including that of clients, suppliers, and staff

Cyber Security Principles

Secure Access

- Systems and devices must be secured using strong passwords and, where possible, multi-factor authentication (MFA).
- Access to data is granted only on a role-specific, need-to-know basis.
- Remote access to company systems is permitted only via secure, encrypted connections.

Device Security

- Company devices and BYOD (Bring Your Own Device) systems must use current antivirus software and be kept up to date.
- All data must be stored on secure, encrypted platforms—typically cloud-based systems that comply with UK GDPR.

Incident Response

- Any breach or suspected breach of data security must be reported to EMC's Data Protection Lead immediately.
- EMC will assess and report notifiable breaches to the Information Commissioner's Office (ICO) within 72 hours, where applicable.

Data Protection Principles

In line with UK GDPR, EMC processes all personal data according to the following principles:

1. Lawfulness, Fairness & Transparency – We only collect personal data for legitimate business purposes and are transparent about its use.
2. Purpose Limitation – Data is collected only for specified purposes and not further processed in a manner incompatible with those purposes.
3. Data Minimisation – We collect only what we need.
4. Accuracy – We keep personal data accurate and up to date.
5. Storage Limitation – We retain data only as long as necessary.
6. Integrity and Confidentiality – We protect data with appropriate security measures.

Signed:

Position: Director
Date: 05/01/25

Privacy Notice

This Privacy Notice explains how EMC uses personal data.

Data Controller: Neil Edwards
Evolution Management Consultancy Lt
Email: info@evolutionmanagementconsultancy.co.uk

Why we collect your data:
We collect and process data for the following reasons:

- To deliver consultancy services
- To communicate with clients and stakeholders
- To manage projects, appointments, and reporting
- To comply with legal obligations

Legal basis for processing:
We rely on one or more of the following legal bases:

- Contractual necessity
- Legal obligation
- Legitimate interest
- Consent (where applicable)

Data retention:
Personal data is retained only as long as necessary for its original purpose or as required by law. Project-related data is usually retained for up to 6 years for audit and compliance reasons.

Your rights:
Under UK GDPR, you have rights including:

- Access to your data
- Correction of inaccurate data
- Erasure ("right to be forgotten")
- Restriction or objection to processing
- Data portability
  To exercise any of these rights, please contact: [Insert contact email]

Third Parties:
We do not sell or share personal data with third parties except where required for service delivery (e.g., secure file sharing with consultants) or to meet legal requirements.

Training and Awareness

All EMC staff and subcontractors are expected to complete annual training in cyber security and data protection. New staff must be trained during onboarding.

Breach Management and Reporting

Any member of staff who suspects a data breach must report it without delay. The breach will be recorded and assessed by the Data Protection Lead. Notifiable breaches will be reported to the ICO and, where required, to the affected data subjects.

Policy Review

This policy is reviewed annually or when significant changes occur in data protection law, cyber risk landscape, or internal systems.

Signed:

Position: Director
Date: 05/01/25