SOUTH EASTERN CARPENTRY

Data Protection Policy

This policy applies to all staff, subcontractors, suppliers, and individuals whose personal data is processed by South Eastern Carpentry Ltd in any format, whether electronic or paper-based.

Principles

- Personal data must be handled according to the seven core principles established by the UK GDPR and Data Protection Act 2018:
- Lawfulness, fairness, and transparency: Data is collected and processed lawfully, fairly, and transparently.
- Purpose limitation: Data is only used for specific, explicit, and legitimate business purposes.
- Data minimisation: Only necessary data is collected.
- Accuracy: Data is kept accurate and up to date.
- Storage limitation: Data is retained only for as long as necessary, with regular reviews and secure disposal.
- Integrity and confidentiality: Technical and organisational measures are implemented to secure data from unauthorised access, disclosure, loss, or destruction.
- Accountability: The company maintains clear records and documentation to demonstrate compliance.

Types of Data Collected

The company processes information relevant to its operations, including:

- Employee information
- Client and supplier details
- Financial and transactional records
- Project and contractual data
- Sensitive information (e.g., health details) where necessary.

SOUTH EASTERN CARPENTRY

Legal Basis for Processing

Personal data is processed under lawful bases such as explicit consent, contract performance, legal obligation, or legitimate interests as specified under GDPR and the Data Protection Act 2018.

Data Subject Rights

Individuals have rights under the GDPR, including:

- Access to their personal data
- Correction of inaccurate data
- Erasure ("right to be forgotten")
- Restriction of processing
- Objection to processing
- Data portability

Requests must be addressed promptly and within statutory timescales.

Data Protection Responsibilities

All employees, subcontractors, and relevant parties must comply with this policy and uphold data protection standards. A designated Data Protection Officer (DPO) oversees compliance, training, and breach management.

Data Security

Appropriate technical and organisational measures, such as access controls, encryption, secure storage, and employee training, are implemented to protect personal data from risks including cybercrime, unauthorised disclosure, and loss. Regular internal inspections and audits will be conducted to ensure ongoing compliance.

Data Sharing and Transfers

Personal data may be shared with internal parties or legitimate external organisations (e.g., government bodies, service providers), but only in accordance with GDPR requirements and company policy. International transfers are subject to additional safeguards.

SOUTH EASTERN CARPENTRY

Data Breach Management

In the event of a data breach, the company will notify the relevant supervisory authority within 72 hours and inform affected individuals if the breach presents a high risk to rights and freedoms.

Review and Updates

This policy is reviewed annually and updated as required to reflect changes in legislation, company operations, or risks.

R. Shroll

Richard Shroll
Managing Director
September 2026