Information Security & Data Protection Policy

Company policy dated 1 January 2025. Rubber-Matting.co.uk edition.

Purpose

This policy sets out Jigsaw Industrial Ltd's commitment to protecting information assets and personal data. We recognise the importance of maintaining confidentiality, integrity, and availability of information to safeguard our business, employees, customers, and suppliers, while complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Information Security Commitments

• Protect all information assets from unauthorised access, disclosure, alteration, or destruction.

• Ensure IT systems and physical records are appropriately secured with access limited to authorised personnel only.

• Maintain business continuity by protecting against loss of data or system outages through backups and secure storage.

• Report and investigate all actual or suspected information security incidents.

• Provide training and awareness so all employees understand their responsibilities for protecting information.

Data Protection Commitments

Jigsaw Industrial Ltd will comply with the principles of UK GDPR, ensuring that personal data is:

1. Lawfully, fairly, and transparently processed.

2. Collected for specific, explicit, and legitimate purposes.

3. Adequate, relevant, and limited to what is necessary.

4. Accurate and kept up to date.

5. Stored securely and only for as long as necessary.

6. Handled with integrity and confidentiality to protect against unauthorised or unlawful processing, loss, or damage.

We will:

• Obtain valid consent where required and respect individuals' data protection rights.

• Limit access to personal data to staff who need it for legitimate business purposes.

• Use secure methods when storing, transferring, or disposing of personal data.

• Only share personal data with trusted third parties under appropriate contractual safeguards.

• Respond promptly to data subject requests (e.g. access, rectification, erasure).

• Notify the Information Commissioner's Office (ICO) and affected individuals of any notifiable data breaches.

Responsibilities

• The Managing Director has overall responsibility for information security and data protection compliance.

• Managers are responsible for ensuring staff in their areas follow this policy.

• All employees must protect information they handle and report security incidents or data breaches immediately.

Review

This policy is communicated to all employees and relevant third parties. It is reviewed annually, or sooner if required by changes in law, regulation, or business practice.