

FIRST Model Management Data Protection Policy

1. Introduction

FIRST Model Management collects and uses personal data relating to customers, suppliers, employees, and business contacts. This policy outlines how data is collected, handled, and stored in compliance with applicable laws.

2. Purpose of Policy

- Ensure compliance with data protection laws
- Protect rights of staff, customers, and partners
- Maintain transparency in data handling
- Reduce risks of data breaches

3. Data Protection Principles

Personal data must:

- Be processed fairly and lawfully
- Be used only for specified purposes
- Be adequate, relevant, and not excessive
- Be accurate and up to date
- Be retained only as necessary (minimum 6 years, except marketing subscribers)
- Be processed in line with individuals' rights
- Be kept secure
- Not be transferred outside the EEA without adequate protection

4. Scope

Applies to all staff, contractors, and stakeholders handling identifiable personal data including names, contact details, and related information.

5. Responsibilities

- Directors: Overall compliance
- Data Protection Manager: Policy oversight, training, subject access requests
- IT Management: System security and monitoring
- Managing Director: Communication approval and external liaison

6. Data Security Guidelines

- Access limited to those who need it
- Use strong passwords
- Do not share data informally
- Keep data updated and securely deleted when no longer needed

7. Data Storage

Paper:

- Store securely in locked cabinets
- Shred when no longer required

Electronic:

- Use secure systems and approved storage
- Encrypt data transfers
- Regular backups and security checks
- Avoid storing data on personal devices

8. Data Usage

- Lock screens when unattended
- Avoid sending personal data via unsecured email
- Use encryption for transfers
- Do not transfer outside EEA

9. Accuracy

- Maintain accurate and updated records
- Avoid duplicate records
- Verify information regularly

10. Subject Access Requests

- Requests via email
- Response within 30 days
- Identity verification required

11. Disclosure

Data may be disclosed without consent where legally required (e.g. law enforcement), subject to verification.

12. Transparency

The company provides a privacy notice explaining how personal data is used and how individuals can exercise their rights.