



Kinetic Systems Support UK Ltd

Building Energy and Control Solutions

Ebenezer House, 605, Bradford Road, Bailiff Bridge, Brighouse,
West Yorkshire, HD6 4DN

Data Protection Policy

Kinetic Systems Support (UK) Ltd

Document Title: Data Protection Policy

Version: 1.0

Effective Date: 26 / 01/ 26

Review Date: 26 / 01/ 26

Approved By: Board of Directors

1. Purpose

This Data Protection Policy sets out how Kinetic Systems collects, uses, stores, shares, and protects personal data in compliance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any other relevant laws.

As a BEMS Systems Integrator , we process personal data relating to employees, customers, suppliers, subcontractors, and other business contacts. We are committed to protecting the privacy and security of this information.

2. Scope

This policy applies to:

- All employees
- Directors and officers
- Agency workers
- Subcontractors
- Consultants
- Temporary staff

- Any third parties processing personal data on behalf of the company

The policy covers all personal data processed by the company, whether held electronically, on paper, or in any other format.

3. Definitions

Personal Data

Any information relating to an identified or identifiable individual.

Examples include:

- Names
- Addresses
- Email addresses
- Telephone numbers
- National Insurance numbers
- Vehicle registration details
- Photographs
- Payroll information

Special Category Data

Sensitive personal information including:

- Health information
- Disability information
- Religious beliefs
- Trade union membership
- Biometric data

Processing

Any operation performed on personal data including:

- Collection
- Storage
- Use

- Sharing
 - Deletion
-

4. Data Protection Principles

The company will comply with the following principles:

Personal data must be:

4.1 Processed Lawfully, Fairly and Transparently

We will only process personal data where we have a lawful basis, including:

- Contract performance
- Legal obligation
- Legitimate interests
- Consent where required

4.2 Collected for Specific Purposes

Personal data will only be collected for legitimate business purposes such as:

- Delivering electrical contracting services
- Managing employees
- Health and safety compliance
- Customer relationship management
- Financial administration

4.3 Adequate, Relevant and Limited

We will only collect data necessary for the purpose for which it is required.

4.4 Accurate and Up to Date

Reasonable steps will be taken to ensure personal data remains accurate.

4.5 Retained Only as Long as Necessary

Data will be retained according to the company's Retention Schedule and legal obligations.

4.6 Kept Secure

Appropriate technical and organisational measures will be implemented to protect personal data.

4.7 Accountable

The company will be able to demonstrate compliance with data protection legislation.

5. Personal Data We Process

Employee Data

The company may process:

- Personal contact details
- Emergency contact information
- Employment records
- Payroll and pension data
- Qualifications and training records
- Driving licence information
- DBS checks (where applicable)
- Health and safety records
- Occupational health information

Customer Data

The company may process:

- Contact names
- Business details
- Site addresses
- Telephone numbers
- Email addresses
- Quotations
- Contracts
- Payment information

Supplier and Subcontractor Data

The company may process:

- Contact details

- Banking information
 - Insurance documentation
 - Certification records
 - Accreditation information
-

6. Roles and Responsibilities

Directors

Directors are responsible for:

- Ensuring compliance with this policy
- Providing adequate resources
- Supporting data protection initiatives

Managers

Managers are responsible for:

- Ensuring staff follow this policy
- Reporting data protection concerns
- Supporting investigations

Employees

Employees must:

- Follow this policy
 - Keep information secure
 - Report data breaches immediately
 - Complete mandatory training
 - Only access information required for their role
-

7. Information Security

The company will implement appropriate security measures including:

Physical Security

- Locked offices and storage areas

- Controlled access to company premises
- Secure disposal of confidential documents

Technical Security

- Password-protected systems
- Multi-factor authentication where possible
- Anti-virus protection
- Firewalls
- Encryption of portable devices
- Secure cloud storage
- Regular software updates

Access Control

Access to personal data will be restricted on a need-to-know basis.

8. Use of Mobile Devices

Employees using company laptops, tablets, or mobile phones must:

- Use strong passwords
- Enable screen locking
- Report loss or theft immediately
- Avoid storing personal data unnecessarily
- Use approved company systems

Personal devices may only be used in accordance with the company's Bring Your Own Device (BYOD) policy.

9. Email and Electronic Communications

Employees must:

- Verify recipients before sending personal data
- Use secure methods when transmitting sensitive information
- Avoid sharing personal data unnecessarily

- Report any accidental disclosures immediately
-

10. CCTV

Where CCTV is used:

- It will be operated for legitimate business purposes
 - Appropriate signage will be displayed
 - Footage will be retained only as necessary
 - Access will be restricted to authorised personnel
-

11. Sharing Personal Data

The company may share personal data with:

- Customers
- Suppliers
- Professional advisers
- Payroll providers
- Pension providers
- Insurers
- Regulatory authorities
- Accreditation bodies

All sharing will be undertaken lawfully and securely.

12. Data Retention

The company will retain information only for as long as required.

Typical retention periods include:

Record Type	Retention Period
Personnel files	6 years after employment ends
Payroll records	6 years

Record Type	Retention Period
Health and safety records	As required by law
Customer contracts	6 years after completion
Financial records	6 years
CCTV footage	Typically 30-90 days unless required for investigation

13. Data Subject Rights

Individuals have the right to:

- Be informed about data processing
- Access their personal data
- Correct inaccurate information
- Request deletion where applicable
- Restrict processing
- Object to processing
- Data portability where applicable
- Not be subject solely to automated decision-making

Requests should be submitted to:

Data Protection Lead: Tim Hardcastle
Email: tim.hardcastle@kineticgroup.co.uk

14. Data Breach Management

A personal data breach may include:

- Loss of documents
- Stolen devices
- Unauthorised access
- Misdirected emails
- Cybersecurity incidents

All breaches must be reported immediately to:

Data Protection Lead: Tim Hardcastle

The company will:

1. Investigate the incident.
 2. Assess risks.
 3. Implement corrective action.
 4. Notify the Information Commissioner's Office (ICO) where required.
 5. Notify affected individuals where necessary.
-

15. Staff Training

The company will provide:

- Data protection awareness training
 - Cybersecurity training
 - Refresher training as required
 - Additional role-specific training where necessary
-

16. Monitoring and Compliance

The company reserves the right to:

- Monitor compliance with this policy
- Conduct audits
- Investigate breaches of policy

Failure to comply may result in disciplinary action and, where appropriate, legal action.

17. Policy Review

This policy will be reviewed:

- Annually
- Following significant legislative changes
- Following major business or operational changes
- Following serious data protection incidents

Approval

Managing Director: Barry Greenwood

Signature: *B Greenwood*

Date: 26 / 01 / 2026
