



Data Protection / GDPR Privacy Policy

A.C. Webb Electrical Contractors Limited ("the Company") is committed to protecting the privacy, confidentiality and security of personal data and to complying with all applicable data protection legislation.

The Company recognises the importance of handling personal information responsibly and is committed to ensuring that personal data is processed lawfully, fairly, transparently and securely.

This policy applies to all employees, subcontractors, supplier's agency workers, consultants and any other persons who process personal data on behalf of the Company.

Policy Statement

The Company is committed to complying with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR), where applicable

The Company will ensure that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified, legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date where appropriate
- Retained only for as long as necessary
- Processed securely and protected against unauthorised access, loss or misuse.

Personal Information We May Process

The Company may collect and process personal information including:

- Name
- Address
- Email address
- Telephone number
- Mobile number
- Business contact details
- Information relating to contracts, quotations and services provided



Personal data will only be collected where there is a legitimate business, contractual or legal reason to do so.

How We Use Personal Data

The Company may process personal data for the following purposes:

- Providing quotations, services and contractual obligations
- Communicating with customers, suppliers and subcontractors
- Managing projects and service delivery
- Maintaining business records
- Meeting legal, regulatory and tax obligations
- Managing employment and subcontractor relationships

The Company will not collect unnecessary personal information and will only process personal data for legitimate business purposes.

Data Security

The Company takes appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, loss or destruction.

These measures may include:

- Password-protected systems
- Controlled access to information
- Anti-virus and cyber security measures
- Secure storage of electronic and paper records
- Secure disposal of confidential information

All employees and subcontractors are expected to maintain the confidentiality of personal information and follow Company procedures relating to data protection.

Data Retention

The Company will retain personal data only for as long as necessary to fulfil the purpose for which it was collected and to meet legal and regulatory obligations.

Where required by law, certain records may be retained for a minimum period, including records required for taxation, accounting and contractual purposes.



When personal data is no longer required, it will be securely deleted or destroyed.

Individual Rights

Individuals whose personal data is processed by the Company have rights under data protection legislation, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (where applicable)
- The right to restrict processing
- The right to data portability (where applicable)
- The right to object to processing
- Rights relating to automated decision making and profiling

Requests relating to personal data will be handled promptly and in accordance with applicable legislation.

Responsibilities

Jason Webb, Managing Director, has overall responsibility for ensuring compliance with data protection legislation and the implementation of this policy.

Employees, subcontractors and any person handling personal data on behalf of the Company are responsible for:

- Complying with this policy
- Maintaining confidentiality
- Reporting any actual or suspected data breaches immediately
- Following Company procedures relating to the collection, use and storage of personal information

Data Breaches

Any actual or suspected data breach must be reported immediately to management.

The Company will investigate all reported breaches and take appropriate action to minimise risks, protect affected individuals and comply with reporting obligations where required.



GDPR Compliance Programme

A.C. Webb (Electrical Contractors) Limited is committed to complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

To support compliance, the Company will:

- Process personal data lawfully, fairly and transparently.
- Collect, use and retain personal data only where necessary for legitimate business purposes.
- Maintain appropriate technical and organisational measures to protect personal data.
- Review data protection arrangements periodically.
- Investigate and respond to data protection incidents and breaches.
- Ensure employees understand their responsibilities when handling personal data.
- Maintain procedures for responding to data subject requests where applicable.

The Managing Director has overall responsibility for ensuring compliance with data protection legislation and Company procedures.

Responsibilities for Handling Personal and Sensitive Data

All employees, subcontractors and persons acting on behalf of the Company who handle personal or sensitive information are responsible for ensuring that such information is:

- Accessed only where necessary for legitimate business purposes.
- Kept secure and protected from unauthorised access, loss, disclosure or misuse.
- Shared only with authorised persons.
- Stored securely in approved systems and locations.
- Disposed of securely when no longer required.



Sensitive information, including employee records, customer information, financial information and any special category personal data, must be handled with particular care and confidentiality.

Any actual or suspected data breach must be reported immediately to management.

Information Technology and Data Security

The Company maintains appropriate information security measures to protect electronic information and personal data.

These measures include:

- Password protection on computers, laptops, tablets and mobile devices.
- Multi-factor authentication where available.
- Firewall protection.
- Anti-virus and anti-malware software.
- Regular software and security updates.
- Secure cloud-based storage and data backup arrangements.
- Restricted access to sensitive information.
- Secure disposal of electronic devices and storage media.

Employees must not share passwords, install unauthorised software or access Company information using insecure systems or networks.

Training and Communication

The Company will provide employees with information, instruction and guidance regarding their responsibilities under this policy.

Data protection awareness will be communicated through:

- Employee induction.
- Policy issue and acknowledgement.



- Management briefings and communications.
- Refresher training where appropriate.
- Cybersecurity awareness training.

Employees are expected to comply with this policy and report any concerns relating to data protection, cybersecurity or information security immediately.

Failure to comply with this policy may result in disciplinary action.

Review

This policy will be reviewed annually and whenever significant changes occur in legislation, company activities, operational risks or organisational structure.

Name: Jason Webb (Managing Director)

Date: June 2026

Review Date: June 2027

Signature: *Jason Webb*