



AC Group – Privacy Notice

1. Introduction

AC Group (“we”, “us” or “our”) is committed to protecting the privacy and personal information of individuals with whom we interact in the course of our business.

This Privacy Notice explains how we collect, use, store, share and protect personal information in accordance with applicable data-protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended from time to time.

This notice applies to individuals whose personal information we process, including:

- Employees, workers and agency workers.
- Job applicants and prospective employees.
- Subcontractors, self-employed contractors and their personnel.
- Clients and prospective clients.
- Suppliers, consultants and professional advisers.
- Visitors and other individuals who interact with our business.
- Other individuals whose personal information we process in connection with our operations.

This notice should be read alongside any separate privacy notice or information we provide for a specific relationship or purpose.

2. Who We Are

For the purposes of data-protection legislation, the relevant AC Group legal entity will generally act as the data controller for personal information it determines the purposes and means of processing.

Organisation: AC Group

Relevant legal entity: AC Electrical (North) Limited

Registered address: AC Group, Riverside Works, Bridge Street, Dukinfield, SK16 4RX **Email:** elicia.simmons@ac-group.co

Telephone: 0161 430 8495

Where different companies within AC Group operate as separate legal entities, the relevant entity responsible for processing your personal information will be identified where appropriate.

For data-protection enquiries, requests or concerns, please contact the HR & Compliance Manager or our designated data-protection contact using the details above.



3. Personal Information We Collect

The personal information we collect will depend on our relationship with you and the purpose for which it is required.

It may include the following categories.

3.1. Identification and contact information

- Name and title.
- Home or business address.
- Telephone number and email address.
- Date of birth, where relevant.
- Identification documents and relevant identification details.
- Emergency contact details, where applicable.

3.2. Employment and recruitment information

- CVs, applications and employment history.
- References and relevant background information.
- Right-to-work information.
- Qualifications, training and professional certifications.
- ECS cards and other competence records.
- Employment contracts and personnel records.
- Working hours, attendance, holidays and sickness absence.
- Payroll, tax, pension and benefits information.
- Performance, disciplinary and grievance records.
- Occupational health and workplace adjustment information, where relevant.

3.3. Subcontractor and contractor information

- Contact and identification details.
- Qualifications, training and competence records.
- ECS cards and other site-access credentials.



- Right-to-work information, where applicable.
- Relevant insurance and business details.
- Working hours and project records.
- Information required by clients, principal contractors, site operators or accreditation bodies.

3.4. Client, supplier and business information

- Business contact details.
- Company and professional information.
- Contractual and project records.
- Correspondence, enquiries and communications.
- Invoice, payment and financial administration records.
- Information required for procurement, supplier management, compliance and contractual obligations.

3.5. Technical and security information

Where applicable, we may process information associated with the use of our systems, devices and premises, including user account details, access logs, security records, online identifiers and CCTV footage where CCTV is operated.

3.6. Special category and criminal offence information

In certain circumstances, we may process special category personal data, such as health information relating to sickness absence, occupational health or workplace adjustments.

We may also process criminal offence information where necessary and legally permitted, for example where relevant checks are required for a particular role or contractual arrangement.

We will only process this information where the applicable legal requirements are met and appropriate safeguards are in place.

4. How We Collect Personal Information

We may collect personal information directly from you, including when you:

- Apply for employment or work with us.
- Enter into a contract or business relationship with us.



- Complete forms or provide identification, qualifications or certificates.
- Communicate with us by telephone, email, post or other channels.
- Visit our premises or attend a project or work site.
- Use systems or services provided by or on behalf of AC Group.

We may also receive personal information from other sources where appropriate and lawful, including:

- Recruitment agencies and referees.
- Previous employers, where relevant and lawful.
- Clients, principal contractors and site operators.
- Subcontractors and their authorised representatives.
- Training providers and accreditation bodies.
- Payroll providers, insurers and professional advisers.
- Public authorities, regulators and other relevant organisations.
- IT, software and other service providers.

Where we obtain personal information from another source, we will provide the privacy information required by applicable law, unless an exemption applies.

5. Why We Use Your Personal Information

We process personal information for legitimate business and operational purposes, including:

- Recruitment, selection and onboarding.
- Managing employment and contractual relationships.
- Administering payroll, pensions, benefits and expenses.
- Managing attendance, absence, performance, training and competence.
- Maintaining health, safety and site-access records.
- Verifying qualifications, certifications and relevant eligibility.
- Managing subcontractors, agency workers, suppliers and clients.
- Delivering and administering contracts and projects.
- Meeting client, principal contractor and accreditation requirements.
- Managing financial records, invoices and payments.
- Maintaining business communications and responding to enquiries.



- Protecting our premises, systems, devices and information.
- Preventing and investigating fraud, misuse and security incidents.
- Complying with legal, regulatory and contractual obligations.
- Establishing, exercising or defending legal claims.
- Maintaining appropriate business, compliance and audit records.

We will only use personal information for purposes that are lawful, fair and compatible with the circumstances in which it was collected, unless further use is otherwise permitted by law.

6. Our Lawful Bases for Processing

We will identify an appropriate lawful basis for processing personal information under the UK GDPR.

Depending on the circumstances, this may include:

Contract: Where processing is necessary to enter into or perform a contract with you, or to take steps you request before entering into a contract.

Legal obligation: Where processing is necessary to comply with a legal obligation applicable to us.

Legitimate interests: Where processing is necessary for our legitimate business interests or those of a third party, provided these interests are not overridden by your rights and interests.

Consent: Where you have given valid consent for a specific purpose. Where we rely on consent, you may withdraw it at any time.

Vital interests: Where processing is necessary to protect someone's vital interests in circumstances permitted by law.

Where we process special category personal data, we will also identify an applicable condition under Article 9 of the UK GDPR and, where required, meet the relevant requirements of the Data Protection Act 2018.

Where we process criminal offence data, we will ensure that an appropriate legal basis and any required safeguards are in place.

The lawful basis will depend on the particular processing activity. We can provide further information about the basis applicable to your personal information where required.

7. Sharing Your Personal Information

We will only share personal information where there is an appropriate lawful basis and the disclosure is necessary and proportionate.

Depending on the circumstances, we may share information with:

- Companies within AC Group, where appropriate and lawful.



- Payroll, pension and HR service providers.
- IT, cloud storage and software providers.
- Occupational health and other relevant healthcare providers.
- Insurers, insurance brokers and professional advisers.
- Accountants, auditors and legal advisers.
- Recruitment agencies and referees.
- Training providers and accreditation bodies.
- Clients, principal contractors and site operators.
- Suppliers and subcontractors where necessary for business operations.
- Banks and payment service providers.
- Government departments, regulators, courts and law-enforcement authorities where required or legally permitted.

We take reasonable steps to ensure that information shared is relevant to the purpose and limited to what is necessary.

Where a third party processes personal information on our behalf, we will put appropriate contractual arrangements and safeguards in place where required.

We do not permit personal information to be used by recipients for purposes that are incompatible with the lawful basis for sharing it.

8. International Transfers

Some of our IT, cloud-based or other service providers may store or process personal information outside the United Kingdom.

Where personal information is transferred internationally, we will ensure that the transfer complies with applicable data-protection legislation. Where required, this may involve an adequacy regulation, appropriate safeguards or another lawful transfer mechanism.

Further information about relevant international transfers and safeguards can be requested using the contact details in Section 2.

9. How We Protect Personal Information

We take appropriate technical and organisational measures to protect personal information against unauthorised or unlawful processing, accidental loss, destruction, damage, alteration or disclosure.

Depending on the information and risks involved, our measures may include:



- Password protection and user access controls.
- Restricting access according to job responsibilities.
- Multi-factor authentication and encryption where appropriate.
- Firewall, antivirus and other cybersecurity controls.
- Software and system updates.
- Secure cloud-based systems and backups.
- Appropriate security arrangements for laptops, mobile phones and other devices.
- Secure storage and disposal of paper records.
- Secure deletion of electronic information.
- Confidentiality requirements and staff training.
- Procedures for identifying, reporting and managing data breaches.
- Periodic monitoring and review of security arrangements.

Employees and other authorised users must only access personal information where they have a legitimate business reason and must follow our policies and procedures.

Although we take reasonable steps to protect personal information, no method of electronic transmission or storage can be guaranteed to be completely secure.

10. How Long We Keep Personal Information

We will retain personal information only for as long as necessary for the purpose for which it was collected, taking account of applicable legal, regulatory, contractual and business requirements.

Retention periods will vary according to the type of information and the circumstances. Factors considered may include:

- Statutory and regulatory requirements.
- Employment, tax and financial recordkeeping requirements.
- Contractual and project obligations.
- Insurance requirements.
- Relevant limitation periods and potential legal claims.
- The rights and interests of the individuals concerned.

We maintain, or will establish where required, appropriate retention arrangements for different categories of personal information.



When information is no longer required, we will securely delete, destroy or anonymise it, as appropriate.

You may contact us if you require further information about the retention period applicable to a particular category of personal information.

11. Your Data Protection Rights

Subject to applicable legal conditions and exemptions, you may have the following rights in relation to your personal information:

Right to be informed: To receive information about how your personal data is collected and used.

Right of access: To request a copy of the personal data we hold about you.

Right to rectification: To request correction of inaccurate or incomplete personal data.

Right to erasure: To request deletion of your personal data in certain circumstances.

Right to restrict processing: To request that we restrict the use of your personal data in certain circumstances.

Right to data portability: To request your personal data in a structured, commonly used and machine-readable format in certain circumstances.

Right to object: To object to certain processing activities, including processing based on legitimate interests and processing for direct marketing.

Rights relating to automated decision-making: To benefit from applicable safeguards where decisions are made solely by automated means and have legal or similarly significant effects.

These rights are not absolute and may be subject to conditions or exemptions under data-protection legislation.

Where we rely on consent, you may withdraw your consent at any time. Withdrawal will not affect the lawfulness of processing carried out before consent was withdrawn.

To exercise your rights, please contact the HR & Compliance Manager or our designated data-protection contact using the details in Section 2.

We may need to verify your identity before responding to a request. We will respond within the applicable statutory timeframe.

12. Subject Access Requests and Other Enquiries

If you wish to access your personal information or make another data-protection request, please contact us using the details in Section 2.

Please provide sufficient information to help us understand your request and identify the relevant records. We may contact you if further information is needed.



We will assess and respond to requests in accordance with applicable legislation, including any relevant exemptions or restrictions.

If you believe that your personal information is inaccurate, has been disclosed incorrectly or is being processed inappropriately, please contact us so that we can investigate the concern.

13. Personal Data Breaches

We maintain procedures for identifying, reporting, assessing and responding to suspected or actual personal-data breaches.

A breach may include the loss or theft of a device containing personal information, an email sent to the wrong recipient, unauthorised access to records or a cybersecurity incident affecting personal data.

Where a breach occurs, we will assess the circumstances and take appropriate action to contain and investigate it, reduce potential harm and prevent recurrence.

Where legally required, we will notify the Information Commissioner's Office (ICO) and affected individuals within the applicable timeframes.

14. Cookies and Website Information

When you visit our website, certain technical information may be processed to operate, maintain and secure the website.

Where our website uses cookies or similar technologies, further information about the technologies used, their purposes and how you can manage your preferences will be provided in an appropriate cookie notice or website privacy information.

15. Changes to This Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in our business activities, systems, data-protection arrangements or applicable legislation.

The current version will be made available through the relevant communication channel, including our website where appropriate.

We encourage you to review this notice periodically to understand how we handle personal information.

16. Complaints and Contact Details

We aim to handle personal information fairly, lawfully and transparently.

If you have a concern about how we use your personal information, please contact:



Data protection contact: HR & Compliance Manager

Organisation: AC Group

Email: elicia.simmons@ac-group.co

Telephone: 0161 430 8495

Postal address: AC Group, Riverside Works, Bridge Street, Dukinfield, SK16 4RX

We will review your concern and respond in accordance with our procedures and applicable legal requirements.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK's independent data-protection regulator, if you are concerned about how your personal information has been handled.

ICO website: <https://ico.org.uk/>

ICO helpline: 0303 123 1113

We would appreciate the opportunity to address your concerns first, although you are entitled to contact the ICO directly.

End of Privacy Notice