

1. Policy Statement

Ecosafe Heating Limited t/a Ecosafe Group requires certain information relating to employees, customers, suppliers, residents and other stakeholders in order to conduct its business operations effectively and lawfully.

The Company is committed to protecting the privacy, confidentiality, integrity and availability of all personal data and will process such information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and all applicable data protection legislation.

This policy applies to all employees, directors, agency workers, subcontractors, consultants and third parties who process personal data on behalf of the Company.

2. GDPR Compliance Programme

Ecosafe Heating Limited maintains an ongoing programme to ensure compliance with UK GDPR requirements. This programme includes:

- Maintaining records of processing activities.
- Identifying and documenting lawful bases for processing personal data.
- Undertaking Data Protection Impact Assessments (DPIAs) where appropriate.
- Managing Subject Access Requests and other individual rights requests.
- Handling data protection complaints.
- Reviewing retention periods and secure disposal arrangements.
- Monitoring compliance with data protection legislation.
- Investigating and reporting personal data breaches where required.
- Reviewing policies and procedures annually.

The Managing Director has overall responsibility for ensuring compliance with this programme.

3. Data Protection Principles

Personal Data includes data in our possession relating to any living individual who can be identified directly or indirectly from that information.

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

Personal Data may be factual, such as a name, address or date of birth, or subjective, such as opinions or assessments relating to an individual.

Personal Data shall be:

1. Processed Lawfully, Fairly and Transparently

Personal Data will only be processed where a lawful basis exists, including:

- Consent of the Data Subject.
- Performance of a contract.
- Compliance with a legal obligation.
- Protection of vital interests.
- Legitimate business interests.

Special Category Data (sensitive personal data) will only be processed where additional legal conditions are met.

2. Collected for Specified Purposes

Personal data shall only be collected for legitimate business purposes and shall not be processed in ways incompatible with those purposes.

3. Adequate, Relevant and Limited

Only the minimum amount of information necessary for the intended purpose will be collected and processed.

4. Accurate and Up to Date

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

5. Retained Only as Long as Necessary

Personal data will not be retained longer than required for legal, contractual or business purposes.

6. Processed in Accordance with Individual Rights

Individuals have rights regarding their personal data, including access, rectification, erasure, restriction, objection, portability and withdrawal of consent.

7. Kept Secure

Appropriate technical and organisational measures will be implemented to protect personal data from unauthorised access, loss, destruction or damage.

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

4. Roles and Responsibilities

Managing Director

The Managing Director is responsible for:

- Approving this policy.
- Ensuring adequate resources are available for compliance.
- Monitoring organisational compliance with UK GDPR.
- Reviewing policy effectiveness annually.

Managers

Managers are responsible for:

- Ensuring employees understand and follow this policy.
- Reporting any suspected breaches immediately.
- Monitoring compliance within their teams.

Employees and Contractors

All employees and contractors are responsible for:

- Handling personal information securely.
- Accessing personal data only when required for business purposes.
- Maintaining confidentiality.
- Recording resident contact details only in the designated contact fields of Company systems, and never in free-text fields (see section 7).
- Reporting suspected breaches immediately.
- Completing mandatory data protection training.

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

5. Information Security and IT Controls

The Company implements appropriate technical and organisational measures to protect personal data.

These include:

- Password-protected systems.
- User access controls based on business need.
- Secure cloud-based systems.
- Firewalls and network security controls.
- Anti-virus and anti-malware protection.
- Software patching and updates.
- Encryption where appropriate.

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

- Secure backup procedures.
- Monitoring of access logs and system activity.
- Secure destruction of electronic and paper records.
- Physical security controls at Company premises.

Only authorised personnel shall have access to personal information relevant to their role.

6. Data Protection Training

The Company provides data protection and information security training to all employees.

Training arrangements include:

- Data protection training during induction.
- Annual refresher training.
- Cyber security awareness training.
- Guidance on recognising and reporting data breaches.
- Training on secure handling of personal and sensitive information.

Training records are maintained and reviewed regularly.

7. Information on Residents

A significant proportion of the Company's work is undertaken within domestic rented properties.

To facilitate appointments, access arrangements and communication during works, the Company receives resident information from customers, landlords, local authorities and housing associations.

In most cases the customer (the local authority, landlord or housing provider) is the data controller for resident information, and the Company processes it as a data processor on the customer's documented instructions and in line with the data protection terms of the relevant contract.

Information held may include:

- Name
- Address
- Telephone number
- Email address

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

- Details of disabilities, vulnerabilities or special access requirements where necessary

Resident personal data is retained for up to 12 months following job completion so that complaints can be handled. It is then removed from the Company's job management system unless an open complaint, defect, claim or the customer contract requires it to be kept for longer.

Resident contact details must only be recorded in the designated contact fields of the job management system. Resident names, telephone numbers, email addresses and details of health conditions or vulnerabilities must not be entered into job descriptions, notes or any other free-text field.

Details of disabilities, vulnerabilities or special access requirements are limited to what is needed to carry out the works safely, and are shared only with the operatives and subcontractors who need them for that job.

A number of historic job records contain resident contact details within free-text fields that cannot be removed without deleting the entire job record. These records are managed under the controls set out in the Outsourced Processing & Cloud Services – PII Protection Policy Addendum (ES-POL-049) and are deleted in full at the end of the job record retention period.

8. Information on Employees

The Company collects and processes employee information for employment, training, health and safety, payroll and operational purposes.

Information may include:

- Name
- Date of birth
- Address
- Telephone number
- Email address
- National Insurance Number
- Next of kin details
- Photographs
- Trade qualifications
- Training records
- Accreditation records
- CSCS card details

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

Where necessary, Special Category Data may also be processed, including information relating to health, disability, religious beliefs, ethnicity or other protected characteristics.

9. Information Collected Through Company Systems

When employees access Company systems or portals, information may be collected including:

- IP addresses
- Login details
- Browser type and version
- Operating system
- Date and time of access
- Usage statistics
- System interaction information

This information is collected to maintain system security, improve functionality and ensure effective service delivery.

10. How We Use Personal Information

Personal information may be used for:

- Administration of employment contracts.
- Payroll and HR administration.
- Recording qualifications and training.
- Resource planning.
- Site access and security management.
- Health and safety management.
- Customer communication.
- Appointment scheduling.
- Legal and regulatory compliance.
- Defending or pursuing legal claims.
- Maintenance of business systems.
- Fraud prevention and security monitoring.

The Company will ensure that any processing remains proportionate and necessary.

11. Lawful Basis for Processing

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

The Company processes personal data using one or more of the following lawful bases:

- Consent.
- Performance of a contract.
- Compliance with legal obligations.
- Legitimate interests.
- Protection of vital interests.

Where consent is relied upon, individuals may withdraw consent at any time.

12. Retention of Information

Personal data will be retained only for as long as necessary to fulfil the purpose for which it was collected.

Resident personal data is retained for up to 12 months following job completion (see section 7). Job records, certificates and reports are retained in line with the Records Protection & Retention Policy (ES-POL-045).

Employment-related records may be retained for up to 15 years where required for legal, insurance or contractual reasons.

At the end of the retention period, information will be securely deleted or destroyed.

13. Disclosure of Information

Personal data may be shared with:

- Business partners and subcontractors.
- Software providers and support providers.
- Professional advisers.
- Auditors.

- Insurers.
- Regulatory authorities.
- Law enforcement agencies.
- Courts and legal representatives.

Information will only be disclosed where lawful and necessary.

14. International Transfers

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

Where personal data is transferred outside the United Kingdom, the Company will ensure appropriate safeguards are in place in accordance with UK GDPR requirements.

15. Individual Rights

Individuals have the following rights:

- Right of access.
- Right to rectification.
- Right to erasure.
- Right to restrict processing.
- Right to data portability.
- Right to object.
- Right to withdraw consent where applicable.

Requests should be submitted to:

Email: info@ecosafegroup.co.uk

The Company will respond within one month where required by law.

Where a request relates to resident data that the Company processes on behalf of a customer, the Company will pass the request to that customer without undue delay and assist the customer in responding.

16. Personal Data Breaches

Any employee who becomes aware of a personal data breach, suspected breach or loss of information must report it immediately to their line manager and the Managing Director.

The Company will:

- Investigate all incidents.
- Record findings and corrective actions.
- Where the breach involves personal data processed on behalf of a customer, notify that customer without undue delay and within any timescale set by the contract.
- Notify the Information Commissioner's Office where required.
- Notify affected individuals where legally necessary.

17. Complaints

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	

If an individual is dissatisfied with the handling of their personal data, they may make a data protection complaint to the Company using the details above. Complaints will be acknowledged within 30 days and investigated without undue delay, and the individual will be kept informed of progress and the outcome.

Individuals also have the right to complain to:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

18. Policy Review

This policy shall be reviewed annually or sooner if:

- Legislation changes.
- Business activities change significantly.
- Security incidents indicate improvements are required.

Signed:



Adam Marston
CEO
Dated: 22/10/2026

Issue: 4	Change Note No: CNN-0082	Review Due: October 2027
Author: A.Marston	Created Date: 23/06/2025	
Approved By: F.Sweetman	Classification: Public	