ideal HEAT SOLUTIONS

POWERING EVERYDAY

DATA PROTECTION POLICY

Rev C

Author:	HR Manager/Managing Director
Date:	February 2026
Person Responsible:	Managing Director
Frequency of Review*:	12 months

** Policies will be reviewed more frequently if legal changes or good practice require, this policy is non-contractual*

Review History		
Date of Review:	Reviewed By	Reason for Review
01/02/2024	**KM/TSS**	New policy
01/02/2025	**LSS/TSS**	Good practice review
01/02/2026	**LSS/TSS**	Good practice review – Some minor amendments

Introduction

In the course of your work with our Company, you are likely to collect, use, transfer or store personal information about employees, clients, customers and suppliers, for example, their names and home addresses. The UK's data protection legislation, including the General Data Protection Regulations (GDPR), contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

The purpose of this policy is to ensure that you are aware that everyone has a responsibility to comply with the principles and legal conditions provided by the data protection legislation, including the GDPR and failure to meet those responsibilities is likely to lead to serious consequences. Firstly, a serious breach of data protection is likely to be a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records or any sensitive personal information without authority, this will constitute a gross misconduct offence and could lead to your summary dismissal. Additionally, if you knowingly or recklessly disclose personal data in breach of the data protection legislation, including the GDPR, you may be held personally criminally accountable for any such breach.

Breach of the data protection legislation, including the GDPR rules, can cause distress to the individuals affected by the breach and is likely to leave the Company at risk of serious financial consequences.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from your Line Manager, HR Manager or hire@idealheatsolutions.co.uk

This policy does not form part of a contract of employment. However, all employees, workers, or contractors must read, understand and comply with the content of this policy. Failure to adhere to this policy is likely to be regarded as a serious disciplinary matter and will be dealt with under the Company's disciplinary rules and procedures.

Definitions

Data Subject: a living individual.
Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.
Data Protection Legislation: The Data Protection Act was replaced in May 2018 by the General Data Protection Regulations (GDPR).

Personal data: is any information that identifies a living individual (data subject) either directly or indirectly. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous, or the identity has been permanently removed, making it impossible to link back to the data subject.

Processing: is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destroying.
Special categories of personal data: this includes any personal data which reveals a data subject's ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.
Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

What are the GDPR principles?

Ideal Heat Solutions Ltd is a data controller. This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during their work with us does so in accordance with the data protection legislation, including the GDPR principles. In brief, the principles say that:

- Personal data must be processed in a lawful, fair and transparent way.
- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up to date.
- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
- The personal data must be kept confidential and secure and only processed by authorised personnel.

Other rules under the GDPR state that:

- The transfer of personal data to a country or organisation outside the EEA should only take place if appropriate measures are in place to protect the security of that data.
- The data subject must be permitted to exercise their rights in relation to their personal data.

The Company and all employees must always comply with these principles and rules in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

What are the lawful reasons under which we would expect you to process personal data?

Whilst carrying out your work activities, you are likely to process personal data. The Company will only expect you to process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

a. Consent has been obtained from the data subject to process their personal data for specified purposes.

b. Where we need to perform the contract, we have entered with the data subject either for employment or commercial purposes.

c. Where we need to comply with a legal obligation.

d. Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where you may need to process the data subject's personal information, these include:

e. Where we need to protect the data subject's interests (or someone else's interests).

f. Where it is needed in the public interest or for official purposes.

You must always ensure that you keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of each processing activity which you perform.

Privacy Notice – Please read the attached Privacy Notice

- Personal data must be processed in a lawful, fair and transparent way.
- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up to date.
- The personal data will not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.

Different categories of personal data will be retained for varying periods, depending on legal, operational, and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed in accordance with its retention of data policy.

- The personal data must be kept confidential and secure and only processed by authorised personnel.

To achieve this, you must follow these steps:

- The Company has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected, ensuring it's protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another employee's records without authority, as this will be treated as gross misconduct and it is also a criminal offence.

- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager.
- Ensure that hard copy personal information is disposed of securely, for example, cross-shredded.
- Manual personnel files and data subject files are confidential and are stored in locked filing cabinets. Only authorised employees have access to these files. For a list of authorised employees, please contact Kelly McNulty. These will not be removed from their normal place of storage without good reason.
- Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked filing cabinets.
- Data held on computers is stored confidentially by means of password protection, encryption or saved on a secure drive.
- The Company has network backup procedures to ensure that data on computers cannot be accidentally lost or destroyed.

The data subject's rights

- The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have several legal rights regarding how their personal data is processed. At any time, a data subject can request that the Company take any of the following actions, subject to certain legal limitations, concerning their personal data:

- Allow access to the personal data
- Request corrections to be made to the data
- Request erasure of data
- Object to the processing of data
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Right to be notified of a data security breach

How should you respond to a data subject request?

- Always verify the identity of the person making a data subject request and the legitimacy of the request.
- If you are unsure as to whether you are authorised to action the request, check the privacy notice to ascertain who is authorised to deal with data subject requests. If you are still unsure how to handle the enquiry, you should contact Kelly McNulty at Ideal Heat Solutions Ltd, Sir Thomas Longley Road, Medway City Estate, Rochester, Kent ME2 4DU or on 01622 933 847.
- If you are authorised to deal with the request, do not give out confidential personal information unless you have received the appropriate consent from the data subject. Seek explicit written consent to process the data subject request and ensure that you keep a clear audit trail of the request and your response.
- Do not share personal information with a third party, unless the data subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not the actual data subject and can include a family member of the data subject.
- Take great care not to accidentally share information with an unauthorised third party.

Be aware that those seeking information sometimes use deception in order to gain access to it.

Categories of information

During your employment, you may be required to process personal data which falls into different categories, general personal data and special categories of personal data. All data should be processed in accordance with the privacy notice and at all times in a confidential manner. However, where that data is classed as a special category, extra care should be taken to ensure the privacy and security of that data. This means that you should maintain a high level of security and you should only share this data with those who are also authorised to process that data. In the context of employee relations, the scenarios when you may be required to process special categories of information may arise for one or more of the following reasons:

- To comply with employment and other laws when processing and managing situations connected with absences arising in relation to sickness or family/dependant-related leave.

- To ensure health and safety obligations and other employment-related obligations are met, you may be required to process information about the physical or mental health or disability status of an employee to assess their capability to perform a role. You may also be required to monitor and manage sickness absence, recommend appropriate workplace adjustments and administer health-related benefits.
- Where it is needed in the public interest, for example, for equal opportunity monitoring and reporting.

We may also require you to process special categories of information in connection with customers and other third parties.

There may also be circumstances where we ask you to process this type of information in relation to assisting the Company with legal claims or to protect a data subject's interests (or someone else's).
You may be asked to process information in relation to criminal convictions. This should be processed
with the highest degree of confidentiality and in accordance with any data protection legislation and privacy notices that are in force in our business.

If you are unsure about how you should process general personal data or special categories of personal data, you must contact your Line Manager or HR Manager.

Exemptions
In limited circumstances, there are certain categories of personal data which are exempt from the GDPR regime. In employment, for example:

- Confidential references that are given, but not those received by the Company from third parties. Only designated Line Managers can give Company references. Confidential references will not be provided unless the Company is sure this is the employee's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Action to be taken in the event of a data protection breach

A personal data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, do not try to handle this yourself.

You must follow the Company's Data Breach Policy, which includes immediately informing your Line Manager so that steps can be taken to:

- Contain the breach.
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

Your Line Manager will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or data subjects need to be notified of the breach.

Training

All employees who handle the personal information of individuals must have a basic understanding of the data protection legislation, including the GDPR. Staff with duties such as computer and internet security, and database management, have been made aware of data protection requirements in their work area.
We will provide you with updates on how to process personal data securely and confidentially and in accordance with the spirit of the data protection legislation, including the GDPR. You will be required to attend all training and to keep yourself informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

Sharing personal data

We may share personal data internally as is necessary. You must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consent. Extra care and security must be

taken when sharing special categories of data or transferring data outside of the Company to a third party.

Complaints

If you believe that this policy has been breached by a colleague or to exercise all relevant rights, queries or complaints, please in the first instance contact your Line Manager at Ideal Heat Solutions Ltd, Sir Thomas Longley Road, Medway City Estate, Rochester, Kent ME2 4DU or on 01622 933 847.

Changes to this policy
We reserve the right to change this policy at any time, so please always check this document regularly to ensure you are following the correct procedures.

This policy was last updated on 01/02/2025

Compliance with GDPR is everyone's responsibility.

By signing this policy, you confirm that you have read and understood the content of this policy, that you agree to adhere to the content and that you understand that breach of any aspect of this policy may lead to serious disciplinary action.

Signed by name of employee/worker/contractor:

Date: