

THT Data Protection Policy

Policy information	
Organisation	<p>TAMWORTH HEAT TREATMENT LTD. 7 DARWELL PARK, MICA CLOSE TAMWORTH, STAFFORDSHIRE. B77 4DR. UNITED KINGDOM.</p> <p>COMPANY REGISTRATION No. 1827957</p>
Scope of policy	To explain how THT will use personal data: how it is collected, how it is held, and how it is processed. It also explains a subject's rights under the law relating to personal data.
Policy operational date	FROM: 06-FEB-2023 TO: 06-FEB-2024
Policy prepared by	MATTHEW WHITEHOUSE, DATA PROTECTION OFFICER.
Date approved by Management on	06-FEB-2023
Policy review date	ANNUALLY. NEXT REVIEW BEFORE 06-FEB-2024

Introduction	
Purpose of policy	<p>The purpose of the policy:</p> <ul style="list-style-type: none"> • complying with the law • following good practice • protecting customers, suppliers, staff and other individuals • protecting the organisation
Types of data	<ul style="list-style-type: none"> • customer contact details • supplier contact details and payment details (bank account / sort code etc.) • employee contact details, including next of kin details, bank details, some medical details <ul style="list-style-type: none"> • Visitor details (name / vehicle Reg / times / CCTV images) • job applicants contact details, employment history, medical info, criminal convictions info
Policy statement	<p>It is our commitment to:</p> <ul style="list-style-type: none"> • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently
Key risks	<p>We identify potential risks as set out below:</p> <ul style="list-style-type: none"> • data on computer systems being stored on personal computers (rather than secure server environment) • staff leaving PC's unlocked and unattended • written data being left exposed (ie on a desk)

THT Data Protection Policy

Responsibilities	
The Board / Company Directors	Kevin Bannister: Managing Director Amanda Crilly: Company Secretary [Director] Matthew Whitehouse: [Director] Daniel Whitehouse: [Director]
Data Protection Officer	Matthew Whitehouse [Director]
Marketing & Customer Relations	Katie Crisp
Employees & Volunteers	All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work
Training	All relevant staff are required to read the guidelines on GDPR as set out by Information Commissioner's Office (ICO.org) And accept they understand it and their role and responsibilities within it.

Security	
Scope	To ensure all relevant data is handled safely and securely at all times and in accordance with the policy
Security measures	<ul style="list-style-type: none"> • No personal data to be kept on individuals PC (only in secure server environment) • All PC's and servers to be password protected • Physical and electronic access to data to be restricted to relevant authorised data processors / controllers • Training for staff regarding phishing emails / web links Send data via email using official company details <ul style="list-style-type: none"> • Administrator Rights restricted to THT IT Manager and ITSLNET (IT supplier). Access authorised by Directors only.
Business continuity	All data is backed up in 2 separate secure physical locations and also online secure back up. Continuous data back up throughout each day, retention / refresh period: 7 days
Specific risks	<ul style="list-style-type: none"> • Phishing emails / web links • Sending data to incorrect recipient (ie via email) • Paper work being left on desks • Leaving PC's unlocked
User Access	Only those with specifically granted access to Admin areas can view confidential data. Access to be decided by MD and IT Director.

THT Data Protection Policy

Data recording and storage	
Accuracy	Where data is taken orally (ie Company data over the phone) then further checks will take place to validate (ie Companies House, VAT register, contact using official registered email address / phone number)
Updating	Customers: annual check of relevant details via questionnaire Suppliers: annual check of relevant details via questionnaire Employees: annual check of relevant details
Storage	Inline with the security aspect of this policy
Retention periods	Customers: Purchase Orders, standard (2 years) (up to 30 years depending on industry sector ie. Aerospace) Suppliers: Invoicing documentation, standard (2 years) Employees: up to 3 years after end of employment
Deletion / destruction	Secure and certified destruction of electronic hardware (ie PC's, servers) and hardcopy documents (ie paper)

Right of Access	
Responsibility	It is the Data Controller that is responsible for ensuring that right of access requests are handled within the legal time limit which is one month
Procedure for making request	To make a request to view / amend / delete any data we hold on file about a person, that person can make a request verbally or in writing using the usual contact details for Tamworth Heat Treatment Ltd. As long as we can positively identify that person, we will release such held data in writing via email or written letter.
Provision for verifying identity	We will verify the identity of that person (making the access request) using a cross reference of the held data and current information given by that person.
Charging	<p>THT will provide the information free of charge. However THT can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.</p> <p>THT may charge a reasonable fee to comply with requests for further copies of the same information.</p> <p>The fee will be based on the administrative cost of providing the information</p>
Procedure for granting access	<p>If the request is made electronically, THT will provide the information in a commonly used electronic format.</p> <p>We do not give access to THT systems for subjects to access the held data.</p>

Transparency	
Commitment	<p>THT's commitment to transparency includes informing subjects;</p> <ul style="list-style-type: none"> • for what purpose data is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	<p>When we obtain data we will inform the subject about our procedures for handling their data, for example via:</p> <ul style="list-style-type: none"> • the handbook for employees • in the welcome letter or Account application form for customers / suppliers • during interviews • on the web site

THT Data Protection Policy

Lawful Basis	
Underlying principles	To be lawful, Fair and transparent. <ul style="list-style-type: none"> • use data only for the purpose stated at the time of obtaining the data • only handle data in ways a subject would reasonably expect • be open and honest, and comply with the transparency obligations of the right to be informed
Opting out	The subject will have the choice to opt out of giving data that it deems is not required
Withdrawing consent	THT acknowledge that, once given, consent can be withdrawn. Although there may be occasions where THT has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn, i.e. ex-employee data is held for 3 years after end of employment.

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data will have their responsibilities outlined during their induction / training procedures
Continuous training	THT will take opportunities to raise Data Protection issues during employee training, team meetings, supervisions, etc.
Procedure for staff signifying acceptance of policy	Written acceptance of an employee's role, responsibilities, understanding and obligations, will be undertaken

Policy review	
Responsibility	THT's Data Protection Officer [Matthew Whitehouse] has the responsibility for carrying out the next policy review
Procedure	All Directors, Data Controllers and some senior management will be involved or informed of the policy review.
Timing	Policy to be reviewed and implemented by the dates shown at the beginning of this policy.