# DATA PROTECTION POLICY

## 1.0 Purpose and aims

The company recognises that it needs to keep certain personal information on its employees, customers, suppliers, etc. to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The company is committed to ensuring any personal data will be dealt with in line with UK Data Protection legislation, including the EU General Data Protection Regulation (GDPR). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

The policy covers all personal data which is held by the company, including data relating to past, present and prospective employees, customers and suppliers.

This policy should be read in conjunction with the IT Policy, the Privacy Notice for Employees, Workers and Contractors and the Document Retention Policy**.**

## 2.0 Definitions

"Personal data" is any information relating to a living individual which is capable of identifying that individual (a "data subject"); such as a name, an identification number, location data, or an online identifier.

The definition of 'processing' is any activity that involves the use of personal data, such as obtaining, using, holding, amending, disclosing, destroying or deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Company will ensure that personal data is:

- Processed lawfully, fairly, and in a transparent manner.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary.
- Processed in a manner that ensures appropriate security of the personal data.
- Not transferred to another country without appropriate safeguards being in place.
- Made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data.

## 3.0 Types of information processed

We process the personal data of individuals who:

- visit our website or interact with us on social media;
- are a supplier (or prospective supplier) to any company within the Group;
- are or have been a customer of any company within the Group;
- are (or work for) a business which might reasonably be expected to have an interest in, or requirement for, the types of products and services that we offer (in other words, a prospective customer)
- are (or have been) employed within the Group, or who have applied for employment.

The types of personal data we process include:

- Employees (past, present, and prospective – i.e., job applicants): name, address, bank account details, national insurance number, telephone number, next of kin details and telephone number, training records. Please refer to the Privacy Notice for Employees, Workers and Contractors for more information.
- Customers (past, present, and prospective): name, address, telephone number, email address, order history, credit references
- Supplier details: name, address, telephone number, email address, bank details for bank transfers.

## 4.0 How do we store personal information

Personal information is kept in the following forms:

- Electronic held on mainframe computer and locally on PCs and laptops;
- Paper records

## 5.0 Responsibilities

The Company has appointed a Data Protection Officer with responsibility for ensuring compliance with this policy. The Data Protection Officer is the Chief Executive Officer (CEO).

The Data Protection Officer will ensure that all employees who process personal information must understand and act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary action being taken and could be considered to be gross misconduct under the company's Disciplinary Procedure.

To meet our responsibilities employees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time the information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

- We will ensure that:
- Everyone managing and handling personal information is trained to do so.
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and professionally.

**6.0 Training**

Training and awareness raising about data protection and how it is applied in this organisation will take the form of general training/awareness. Employees who regularly process data will, on a regular basis, be reminded about their responsibilities under the Data Protection legislation and be asked to complete refresher training.

**7.0 Gathering and checking information**

Before personal information is collected, we will:

- Consider what details are necessary in order to adequately complete our purpose;
- Identify how long this information will need to be kept to comply with other legislation and business need.

We will inform people whose information is gathered about the following:

- Why the information is being gathered;
- What the information will be used for;
- How the information will be stored;
- Who will have access to the personal information.

We will take the following measures to ensure that personal information kept is accurate:

- Annually sending out requests for employees to update their records;

Personal sensitive information will not be used for any purpose other than the exact purpose for which permission is given.

**8.0 Data Security** [see also the IT Policy]

We will take steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Keeping paper records stored in lockable cabinets;
- Computer systems having protected personal access passwords;
- Data back-ups to be kept on site:

Any unauthorised disclosure of personal data to a third party by an employee may result in action being taken under the Disciplinary Procedure.

## 9.0 Retention of Personal Information

Personal information will only be retained for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are available in our retention policy which is available on the Intranet or from the Human Resources department. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data, the purposes for which we process personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We will retain and securely destroy personal information in accordance with our Document Retention policy.

## 10.0 Subject Access Requests

Anyone whose personal information we process has the right to request a copy of their personal data. Any such request must be dealt with promptly (it is our policy to respond within 28 days).

In certain circumstances, individuals have the right to:

- Have inaccurate personal data corrected
- Have personal data erased ("the right to be forgotten")
- Object to the processing of personal data
- Restrict the processing of personal data
- Receive the personal data they have provided to us in a machine-readable format or have it transmitted directly to another data controller

A Subject Access Request may be made verbally or in writing and does not have to be made formally to any specific person within the Company. Therefore, any employee receiving what they think may be a Subject Access Request, or a request to exercise any of these rights, must notify their Line Manager and the Data Protection Officer immediately.

Any employee wishing to exercise any of these rights in respect of their own personal data is requested to notify their local HR Department.

In order to consider any Subject Access Request, we will require the following information and we may also require proof of identity.

- Full name and contact details of the person making the request
- Their relationship with the organisation;
- Presentation of appropriate personal identification, e.g., passport, birth certificate or photo card driver's licence.

Where we believe a request to be excessive or unfounded, we reserve the right to charge an administration fee.

**11.0 Right to Withdraw Consent**

In the limited circumstances where an individual has provided consent to the collection, processing and transfer of their personal information for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. To withdraw consent, please contact the Data Protection Officer. Once we have received notification that consent has been withdrawn, we will no longer process personal information for the purpose or purposes originally agreed to, unless we have another legitimate basis for doing so in law.

**12.0 Personal Data Breach**

Full details of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, must be notified to the Data Protection Officer immediately it is discovered. Personal data breaches could include:

- Access by an unauthorised third party
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- A ransomware attack resulting in all data being encrypted.
- A direct marketing email is sent in such a way that recipients can view the email address of all other recipients.

This Policy will be reviewed on a regular basis to ensure it remains up to date and compliant with the law.

*Last updated: January 2022*