



Data Protection Policy

The Company is committed to comply with the requirements of the Data Protection Act 2018 that govern the processing of personal data. Consequently, personal information will be collated and used fairly, stored safely and not disclosed to any other person unlawfully.

Personal data can be defined as data or information relating to an individual from which they can be identified, and which can include expressions of opinion about an individual. The company's aims are to ensure that personal data is not used for any other purposes than specified on collection, is held securely, and destroyed when no longer required.

Individual Staff also have a responsibility to ensure that data is processed correctly and lawfully – this is fully outlined in section 4 of this policy

If at any point you are concerned that we are not complying with Data Protection rules you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Section 1: Data Protection Principles

The Company recognises the importance of safeguarding personal privacy when dealing with information about Data Subjects:

- Personal Data will be processed fairly and lawfully and in line with advice from the Information Commissioner;
- Personal Data will be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- Personal Data will be accurate and, where necessary, kept up to date;
- Personal Data shall not be kept for longer than is necessary for the purposes for which it is obtained;
- Personal Data shall be processed in accordance with the rights of Data Subjects;
- Appropriate measures will be taken against unauthorised or unlawful processing of Personal Data and against its accidental loss, damage or destruction; and
- Personal Data shall not be transferred to a country outside the European Economic Area (the "EEA"). If at any point this changes we will ensure that this is done in compliance with the law

Section 2: The Data we hold

We hold personal data for 3 distinct groups of individuals

a) Current and past employees

We hold data on you, including:

- Name and address
- Bank Details
- Identification documents (such as passport details)
- Contractual Documents
- Specific personal details such as sex, race, disability
- Employment history with the company (including absence records, disciplinary and grievance issues etc)
- Use of our IT systems (emails, web browsing etc)
- Tracking data from company vehicles
- CCTV images from our site security
- Photos used for security badges/ID

All of this data is retained securely, and we hold either because we are required to do so by law or because we have legitimate interests to do so (for example to pay you correctly, to ensure we are complying with our responsibilities as an employer, or because it is necessary to run the business effectively)

After you leave the company, we will retain all your data for at least 180 days, after which we start to delete certain aspects. We are required by law to retain some of your data for defined periods (e.g. we need to retain tax information for 6 years) and in some cases we need to hold this indefinitely (certain health and safety information).

b) Job Applicants

If you apply for a job with the company, and are unsuccessful, we will retain your application details (CV etc) for a period of no more than 6 months after the vacancy has been filled.

c) Customers and Suppliers

Personal information relating to individuals employed by our customers or suppliers will be processed in accordance with the principles above and will not be retained once there is no longer any legitimate business to do so (for example, if we no longer have a commercial relationship with the company, or the individual no longer works for them or is no longer involved in the management of the commercial relationship)

We will seek explicit consent to hold personal data for marketing purposes.

Section 3: Rights of Data Subjects

Data Subjects can be defined as individuals who are the subject of personal data. All data subjects are entitled to know:

- what information the company holds and processes about them and why.
- how to gain access to it, and,
- how to keep it up to date.

You may request this information by contacting the company. There is no charge for doing this and we will respond to your request within the timescales laid down in law.

However you should be aware that the company may make a charge, or refuse to deal with your request, if you make frequently repeated requests or your request is manifestly unfounded.

While we will do everything possible to protect your data, in the event of a breach we will do everything required to rectify the situation, including where necessary inform the Information Commissioner.

Section 4 - Employees' Responsibilities

It is your responsibility to ensure that any data you deal with is held securely and is only accessible to those who have a legitimate business reason to have it

Personal data should never be removed from our premises, unless you have been authorised by a director to do so.

You must follow basic security such as

- a) Never leave papers on your desk or in a vehicle
- b) Lock drawers containing personal data
- c) Ensure your computer screen is locked when you are away from your desk
- d) If you 'hot desk', ensure that you log off any computers and remove any documents before leaving the desk
- e) In particular, if you are hosting visitors from another organisation you are responsible for ensuring that they are not able to see or access any personal data (both in paper or computer format) unless authorised to do so.
- f) Password protect any attachments containing personal data before sending them via email.
- g) Never transfer personal data to a memory stick or other removeable device

If you become aware of any type of data breach, you must inform your manager immediately.

If you are working from home, or any other location outside our office, you must ensure that you only use our IT services to access and/or save information. You must not save any personal data on your own IT equipment.

If you breach any of these data protection rules we may consider it a disciplinary matter. A serious breach could be considered as gross misconduct.