This is the Company's policy and statement in relation to data protection.

In order to operate, the Company needs to collect and use certain types of information about the people with whom it deals. These include current, past and prospective employees, clients, suppliers and others with whom it communicates. This personal information must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer or recorded on other material and certain safeguards are in place to ensure this has been done in accordance with the General Data Protection Regulation (GDPR) 2018.

We take the issue of data protection very seriously and regard the lawful and correct treatment of personal information with the utmost importance to guarantee the successful operation of the Company and to maintain the confidence of those with whom we deal.

To this end, the Company fully endorses and adheres to GDPR and its data protection principles therefore all data will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

It is the duty of all employees to ensure that they are fully aware of this policy and that they comply with its directions. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Processing Personal Data

In the course of their employment some employees will have contact with a variety of confidential and sensitive personal data belonging to our clients and other employees who work for the Company from time to time.

"Personal Data" is data about a living individual who can be identified: -

- Come into the possession of the Company.
- Individuals about whom personal data are kept are known as "data subjects" and an organisation that holds and uses or processes data (as the Company does) is called a "data controller".

Employees will process personal data when they obtain, record, read, hold or use personal data. All of the following activities will constitute the processing of personal data (without limitation): -

- Obtaining, filing, adapting or retrieving data
- Consulting with someone on the content of data or otherwise using it
- Disclosing data by transmitting it, disseminating it or otherwise making it available (including disclosures made to other employees or clients)
- Combining the data with other data
- Erasing or destroying data.

Personal data must be processed in accordance with GDPR principles to which we will make all reasonable efforts to adhere.

The personal data processed in the course of employment must not be disclosed to any person or other employees or outside the Company other than to a business or trading partner or otherwise than in the proper performance of employee's duties either during their employment by the Company or after the termination of their employment. Any disclosure of personal data not authorised by the individual whom it concerns, a partner or by law, or any other authorised use of personal data by employees could result in disciplinary action being taken against employees for misconduct or gross misconduct.

Under GDPR the company will only process personal data for one of six lawful reasons namely:

- Contractual necessity - fulfil contractual obligations; or because they have asked you to do something before entering into a contract (e.g., provide a quote).
- Legitimate interests – the need of the company is greater than the data subjects.
- Consent – explicit written consent given by the data subject to hold the personal data.
- Compliance with a legal obligation – the processing of personal data to comply with a common law or statutory obligation.
- Vital interests – if the data subject is not capable of giving consent but it is in their best interests i.e. in a life of death situation.
- Administering justice/public interest – relevant to public authorities.

Consent

If the company is relying on consent to process personal data this consent must be freely given, have a specific and clear statement and name any third parties with access to the data. Data subjects can withdraw this consent at any time. Any employee's wishing to do so must contact HR, any customers or potential customers must contact the marketing department.

The Company will inform individuals if it is processing their personal data, this information will be concise, transparent, intelligible, easily accessible, and in clear and plain language.

Individuals may access the personal data held by the company free of charge. This will be provided within one month of receipt of the request. Unless it is particularly complex request or there have been numerous requests, in which case the company will inform the individual within one month that the timescale has been extended by a further two months.

If any information held is incorrect individuals have the right to have personal data rectified, or completed if it is incomplete. This request can be made verbally or in writing. The company will respond to a request within one month.

Individuals have the right to request data to be erased or restricted if it is no longer necessary. The company will respond to any such requests within one month.

If individuals object to personal data being held on "grounds relating to his or her particular situation" the company will stop processing it unless:

- compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual can be demonstrated; or
- the processing is for the establishment, exercise or defence of legal claims.

If the data is used for direct marketing purposes the company will stop processing the personal data immediately.

Handling and Storing Personal Data and Data Security

As identified above, the Company is obliged to ensure that personal data is secure. The appropriate level of security must be established having regard to the type of personal data being processed, the likelihood of disclosure and the harm that may result from any breach of security. Therefore, particular care should be taken of records which have a particular sensitivity such as clients' files and employment records.

To safeguard against any unauthorised access to personal data in the company's possession, all employees will take steps to ensure that the personal data is kept secure. It is important to recognise that information will not always be secure simply by virtue of being within the confines of our offices and special care must be practised when taking files containing personal data outside the office environment.

Particular care will also be taken to ensure that personal data is properly and securely disposed of.

We may transfer personal data to insurers, payroll, bankers, legal, medical and other professional advisers, administrators of our pension scheme and other companies to which we have contracted work relating to any of the above purposes for which the personal data is to be used. The company will ensure that any such information passed on to third parties is secure and that those third parties data protection policies comply with GDPR.

Individuals have the right to request to obtain and reuse their data, any such request will be responded to within one month. If the request is complex or there have been numerous request this can be extended a further 2 months. If an extension is needed the company will inform the individual within one month.

Processing of Employees Personal Data

In the course of recruitment and employment, we will collect, hold and process information consisting of personal data including sensitive personal data (see below) about all our employees, applicants for employment, self-employed contractors, agency workers and others who work for us, who are referred to in the Act as "data subjects".

The information we hold is as follows listed under the lawful basis for holding the data: -

Performance of Contract

- full name
- address and postcode
- telephone number/s and personal email address
- date of birth
- bank Details
- national Insurance number
- remuneration, tax, NI other deductions, benefits and pension details
- periods of holiday, sick leave and family or other leave
- work schedule and attendance and overtime records.

Compliance of a Legal Obligation

- payroll number
- driving licence information
- notice for impending prosecutions (driving)
- data obtained from the trackers fitted to company vehicles
- records of health and safety incidents
- details of nationality and eligibility to work in the UK.

Legitimate Interest

- contract of employment
- emergency contact details
- career history including start and end dates with the company and former employers, and promotions
- relevant medical records e.g., reasons for absence, details of doctors, dentists and hospital appointments, GP reports or notes, occupational health advice, details of disabilities that may require reasonable adjustments
- application forms, C.V., interview records and references
- appraisals and other performance measures/monitoring
- training
- beneficiary contact details
- discipline and grievances
- drug and alcohol testing

Sensitive Personal Data

We will also hold certain data about the persons described above which is defined by GDPR as "sensitive personal data" such as: -

- race
- ethnic origin
- politics
- religion
- trade union membership
- health
- sex life
- sexual orientation.

To process this data the company must have a lawful basis for processing and need to satisfy a specific reason outlined below: -

- The company has explicit consent from the data subject
- Necessary in the obligations for employment
- Necessary for the assessment of the working capacity

Retention Periods for Personal Data

The categories of information which we will hold and the time for which we will normally hold it will be as follows in accordance with the Code of Practice published by the Information Commissioner-

Application Form	Duration of Employment.
References received	1 year.
Payroll and tax information	6 years.
Sickness records	3 years.
Annual leave records	2 years.
Unpaid leave/special leave records	3 years.
Annual appraisal/Assessment records	5 years.
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment.
References given/information to enable reference to be provided	5 years from reference/end of employment.
Summary of record of service (e.g., name, position held and dates of employment	10 years from end of employment.

Records relating to accident or injury at work	12 years.

The purpose for which we hold any information about data subjects after the end of employment (as indicated in the above table) is for use solely for any residual employment related matters including (but not limited to) the provision of job references, processing applications for re-employment, matters relating to retirement benefits and allowing us to fulfil contractual or statutory obligations.

Other Data Processed

We monitor electronic communications by employees including to websites and emails, to ensure that these systems are being used in accordance with our Email and Internet Access Policy.

All branches are monitored by CCTV footage for security and health & safety purposes. Any individuals entering a branch either as a customer, supplier, visitor or employee will be recorded on the CCTV system. This footage will be stored for no longer than 2 months unless there has been an incident. In this case the footage will be downloaded and stored until it is no longer required.

Review

This policy will be reviewed annually and revised where it is considered appropriate to do so having regard to legislative change.

This policy does not form part of an employee's contract of employment and can therefore be amended at any time.

Date: 1st January 2024