DATA PROTECTION POLICY

This policy sets out the Company's obligations with regards to data protection and the rights of people with whom it works in respect of their personal data under the General Data Protection Regulation (EU) 2016/679 ("the Regulation").

The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties and its employees. The Company shall ensure that it handles all personal data correctly and lawfully.

Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data:

(a) Must be processed fairly, lawfully and in a transparent manner (and shall not be processed unless certain conditions are met);

(b) Must be obtained only for specified, explicit and legitimate purposes and shall not be processed in any manner which is incompatible with those purposes;

(c) Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;

(d) Must be accurate and, where appropriate, kept up-to-date;

(e) Must be kept in a form which permits identification of data subjects for no longer than is necessary in light of the purpose(s) for which it is processed;

(f) Must be processed in a manner that ensures appropriate security for the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures;

(g) Must be processed in accordance with the rights of data subjects under the Regulation;

(h) Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Rights of Data Subjects

Under the Regulation, data subjects have the following rights:

- The right to be informed that their personal data is being collected and processed and with whom it is being shared;

- The right to access any of their personal data held by the Company within one calendar month of making a request;

- The right to prevent the processing of their personal data in limited circumstances; and

- The right to have incorrect or incomplete personal data rectified, blocked, erased or destroyed, within one calendar month of making the request;

- The right to erasure, blocking or restricting of the processing of personal data, within one calendar month of making the request;

- The right to move, copy or transfer personal data from one IT environment to another in a safe and secure way without hindrance or usability;

- The right to object to the processing of their personal data in certain circumstances;

- The right not to be subject to automated decision making unless necessary for the performance of a contract between the data subject and the Company; the Company is authorised by law or the Company has received the explicit consent of the data subject.

If you would like to exercise any of those rights or you receive a request from a customer or supplier that they wish to exercise any of those rights, please:

- Email, call or write to us;
- Let us have enough information to identify you or the customer or supplier;
- Where the request relates to your personal data, let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
- Let us know the information to which your request or the request of a customer or supplier relates

Personal Data

Personal data is defined by the Regulation as data which relates to an identifiable person who can be directly or indirectly identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Regulation also defines “sensitive personal data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their genetic or biometric data; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any Court in such proceedings.

As regards its employees, the Company only holds personal data which is directly relevant to the employment contract. That data will be held and processed in accordance with the data protection principles and with this Policy. The following data may be collected, held and processed by the Company:

- Identification information relating to employees including, but not limited to, names and contact details, passport information, signatures, photographs;

- Equal opportunities monitoring information including age, gender, race, nationality and religion;

- Health records including details of sick leave, medical conditions, disabilities and prescribed medication;

- Employment records including, but not limited to, interview notes, curricula vitae, application forms, assessments, performance reviews and similar documents, Disclosure and Barring Service records;

- Details of salaries including increases, bonuses, commission, overtime, benefits and expenses;

- Records of disciplinary matters including reports and warnings, both formal and informal;

- Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes;

Health Records

The Company holds health records on all employees which are used to assess the health, wellbeing and welfare of employees and highlight any issues which may require further investigation. Such health records will include details of sick leave, medical conditions, disabilities and prescribed medication. Data under this heading will be used by management only and will not be revealed to fellow employees and peers (unless those employees are responsible for health records in the normal course of their duties).

Employees have the right to request that the Company does not store health records. All such requests must be made in writing and addressed to the Human Resources Adviser.

Monitoring

The Company's systems enable us to monitor telephone (including mobile telephone), email, voicemail, internet and other communications. Any individual's use (including personal use) of our systems may be monitored by automated software or otherwise, for business reasons, in order to carry out our obligations as an employer and in order to monitor compliance with the terms of this policy.

The Company reserves the right to monitor, intercept, retrieve and read the contents of any internal or external email or other communication**,** to listen to or record any telephone conversation or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the Company's business, including for these purposes (the list is not exhaustive):

- monitoring and record keeping to establish facts;
- to establish compliance with regulatory or self-regulatory procedures;

- to prevent, detect or investigate alleged crime or wrongdoing;
- to investigate or detect the unauthorised use of the Company's systems or to ascertain compliance with the Company's policies, practices or procedures (including this policy);
- to locate and retrieve lost messages or files;
- to check whether communications are relevant to the business (for example when an individual is absent due to sickness or holiday); and/or
- to comply with any legal obligation.

The Company may from time to time monitor the activities of employees. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. Any employee that is to be monitored shall be informed in advance of such monitoring where applicable.

Under no circumstances will monitoring interfere with an employee's normal duties.

The Company shall use its best and reasonable endeavours to ensure that there is no intrusion upon employees' personal communications or activities and under no circumstances will monitoring take place outside of the employee's normal place of work or work hours.

The Company also tracks and monitors the location of its Company vehicles. Data gathered in this fashion will be processed in accordance with the Company's Company Vehicle Policy.

Processing Personal Data

Any and all employees' personal data collected by the Company is collected in order to ensure that the Company can efficiently manage its employees and conform with its equal opportunities obligations. Personal data shall also be used by the Company in meeting any and all relevant obligations imposed by law.

We may collect this information from you, your personnel records and recruitment agencies.

We use your personal information:

- For the performance of a contract with you, or to take steps to enter into a contracts;
- For compliance with a legal obligation (eg our obligations to you as your employer under employment protection);
- To comply with our customer and supplier contracts; and
- For the purposes of our legitimate interests or those of a third party, but only if these are not overridden by your interests, rights or freedoms.

Personal data may be disclosed within the Company. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data in view of the purpose(s) for which it was collected and is being processed.

We routinely share your personal data, notably your name, position and address with our legal advisors and insurance provider. We may also use your personal data for reference purposes on tender bids and for marketing purposes. This data sharing enables us to manage your employment with us; to advance the marketability of the Company and to comply with our Legal and Insurance obligations.

We will share personal information with law enforcement or other authorities if required by applicable law.

We will not share your personal information with any other third party.

We will hold your personal data in accordance with our records management policy which should be read in conjunction with this Policy.

We may transfer your personal information to countries located outside the European Economic Area (EEA)

Such countries do not have the same data protection laws as the United Kingdom and EEA. Any transfer of your personal information will be subject to suitable safeguards (as permitted under the General Data Protection Regulation that are designed to help safeguard your privacy rights and give you remedies in the unlikely event of a misuse of your personal information.)

The Company shall ensure that:

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully;
- Employees are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s);
- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed;
- No personal data is held for any longer than necessary in light of the stated purpose(s);
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred using secure means, electronically or otherwise;
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory; and
- All employees can exercise their rights set out above and more fully in the Regulation.

Data Protection Procedures

The Company shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company comply with the following and the Company's Information Security and Record Management Policy when processing and / or transmitting personal data:

- All emails containing personal data must be encrypted;
- Personal data may be transmitted over secure networks only – transmission over unsecure networks is not permitted in any circumstances;
- Where personal data is accessed remotely by an authorised personnel, this must be over a secured network and only where the data is suitably encrypted;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient. Using an intermediary is not permitted;
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar with access restricted to those authorised personnel;
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet with access restricted to those authorised personnel;
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised;
- Where personal data is processed for the purpose of marketing by the Company, pseudonyms will be used where possible subject to the consent of the data subject;
- Any processing of customer personal data will be in accordance with the Company's Privacy Policy.

Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A designated officer ("the Data Protection Officer") within the Company shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Regulation.

- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company are made fully aware of both their individual rights and responsibilities and the Company's responsibilities under the Regulation and shall be furnished with a copy of this Policy and the Company's Information Security and Record Management Policy.

- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.

- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be appropriately supervised.

- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.

- All personal data shall be kept up-to-date and in accordance with the Information Security and Record Management Policy. If an employee's personal data changes the employee shall be under a duty to inform the Human Resources Department of those changes.

- Any personal data which is older than [5] years or no longer required shall be deleted or otherwise destroyed.

- The performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.

- All employees, contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy.

- Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Regulation.

- All contractors, agents, consultants, partners or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation.

- Where any contractor, agent, consultant, partner or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Access by Data Subjects

A data subject may make a subject access request ("SAR") at any time to see the information which the Company holds about them.

SARs can be made in writing (including e-mails or other electronic means) and no charge can be made by the Company to respond to an SAR.

Upon receipt of a SAR the Company shall have up to one calendar month within which to respond. The following information will be provided to the data subject:

- Whether or not the Company holds any personal data on the data subject;
- A description of any personal data held on the data subject;
- Details of what that personal data is used for;
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.