Data Protection Policy

INTRODUCTION:

The General Data Protection Regulations (GDPR) protects employees against the misuse of personal data and may cover both manual and electronic records.

All records whether they be held electronically or physically fall within scope of the Regulations.

The Regulations require that any personal data held should:

a. be fairly and lawfully processed

b. be processed for limited purposes and not in any manner incompatible with those purposes

c. be adequate, relevant and not excessive

d. be accurate

e. not be kept for longer than is necessary

f. be processed in accordance with individuals' rights

g. be secure; and

h. not be transferred to countries without adequate protection

The Regulations also give employees certain rights. For employment purposes, the most important right is the right to access personal data held about the employee.

POLICY:

In the course of your employment you may come into contact with and use confidential personal information about clients and employees, such as names and addresses or even information about personal circumstances, families, health and other private matters. This policy helps you ensure that you do not breach the General Data Protection Regulations, which provides strict rules in this area (as outlined above). If you are in any doubt about what you may or may not do seek advice from your line manager.

The company holds personal data about you. A privacy notice will be provided separately which tells you what information we hold, what we do with it, who we share it with and the lawful basis for the processing of your data. If this information changes you should let us know at the earliest opportunity so that our records can be up-dated.

The personal data that has been collected about you will be kept for the following purposes:

a. recruitment, promotion, training, redeployment and/or career development

b. administration and the payment of wages

c. calculation of certain benefits, including pensions

d. disciplinary or performance management purposes

e. performance review

f. recording of communication with employees and their representatives

g. compliance with legislation

h. provision of references to financial institutions, to facilitate entry onto education courses and/or to assist future potential employers; and

i. staffing levels and career planning

The company considers that the following personal data falls within the categories set out above:

a. personal details, including name, address, age, status and qualifications

b. references and CVs

c. emergency contact details

d. notes on discussions between management and the employee

e. appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment

f. training records

g. salary, benefits and bank/building society details; and

h. absence and sickness information

The company will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

Subject to the aforementioned annual review, information collected will be retained throughout the duration of the employee's employment. After termination of employment, information collected will be reviewed and where there is no business reason for keeping the information, the information will be securely destroyed.

Employees information will be held for the statutory retention period as outlined in the table below:

Record	**Statutory Retention Period**
Accident Reports	Three years after date of last entry. These are rules on recording incidents involving hazardous substances
Payroll Records	At least three years after the end of the tax year they relate to
Statutory Maternity, Adoption and Paternity Pay Records	Three years after the end of the tax year they relate to
Statutory Sick Pay Records	Three years after the end of the tax year they relate to
Working Time	Two years' from date on which they were made
National Minimum Wage Records	Three years after the end of the pay reference period following the one that the records cover
Retirement Benefits Schemes- Notifiable events, e.g. relating to incapacity	Six years from the end of the scheme year in which the event took place
Application forms/interview notes for unsuccessful candidates	One year
Health and Safety records of consultations	Permanently
Parental leave taken	Five years from birth/adoption, or until child is 18 if disabled
Pension records	Six years
Disciplinary, working time and training records	Six years after employment ceases
Redundancy details	Six years from date of redundancy
Senior executives' records	Permanently for historical purposes
Trade union agreements	Ten years after ceasing to be effective
Minutes of trustee/ work council meetings	Permanently
Eligibility to work documents	Two years after employment ceases

However, in exceptional circumstances this information may be held for longer periods and in this case the company will explain the legal basis for retaining the data upon request.

The employee has the right to request that their personal data is deleted; such requests will be dealt with by the Compliance manager, who will review the request and take appropriate steps. If the request is denied, the company will respond with the company's reasons, including the legal basis, for retaining data.

SPECIAL CATEGORY DATA

Special category data includes information relating to the following matters:

a. the employee's racial or ethnic origin

b. his or her political opinions

c. his or her religious or similar beliefs

d. his or her trade union membership

e. his or her physical or mental health or condition

f. his or her sex life; or

g. the commission or alleged commission of any offence by the employee

To hold special category data, the company must additionally satisfy a special category data condition. The most appropriate condition for employment purposes is that the processing is necessary to enable the company to meet its legal obligations (for example, to ensure health and safety or to avoid unlawful discrimination).

ENSURING OUR COMPLIANCE

For information on GDPR and your obligations, or if you have any concerns you should contact the Compliance Manager.

Employees who have access to personal data must comply with this Policy and adhere to the procedures as laid down. Failure to comply with the Policy may result in disciplinary action up to and including summary dismissal.

USE OF PERSONAL DATA

To ensure compliance with the Regulations and in the interests of privacy, employee confidence and good employee relations, the disclosure and use of information held by the company is governed by the following conditions:

a. personal data must only be used for one or more of the purposes specified in this Policy

b. company documents may only be used in accordance with the statement within each document stating its intended use; and

c. provided that the identification of individual employees is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external request for data (for example, surveys, staffing level figure); and

d. personal data must not be disclosed, either within or outside the company, to any unauthorised recipient

PERSONAL DATA HELD FOR EQUAL OPPORTUNITIES MONITORING PURPOSES

Where personal data obtained about candidates is to be held for the purposes of equal opportunities monitoring, all such data will remain anonymous.

ACCURACY OF PERSONAL DATA

The company will review personal data regularly to ensure it is accurate, relevant and up to date.

In order to ensure the company's files are accurate and up to date, and so that the company is able to contact the employee or, in the case of an emergency, another designated person, employees must notify the company as soon as possible of any change in their personal details.

These records will be stored in the employee's personnel file.

ACCESS TO PERSONAL DATA ('SUBJECT ACCESS REQUEST')

Employees have the right to access personal data held about them. The company will arrange for the employee to see or hear all personal data held about them within 30 days of receipt of a written request. A Subject Access Request form can be obtained from your line manager. Information will be provided electronically in a commonly used format.

DATA BREACHES

Where the company becomes aware of a personal data breach it will, without undue delay and where feasible, not later than 72 hours of becoming aware of it, notify the personal data breach to the ICO, unless the controller is able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the above aim cannot be achieved within 72 hours, an explanation of the reasons for delay will accompany the notification to the ICO and information may be provided in phases without undue further delay. In addition, data subjects will be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms to allow them to take the necessary precautions. This notification will describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. This will be done as soon as reasonably feasible, and in close co-operation with the ICO.

Signed: Stephen Holmes
Managing Director

Date: 17/08/2018