Information is a valuable asset within the organisation and therefore needs to be suitably protected. It exists in many forms: electronic, visual, hard copy or verbal. Information can be received by the company and leave the company by many routes and be stored in many forms.

Whatever form the information is in (or however stored or transmitted) the information security measures taken within the company ensure that it is accessible to, and usable by, the appropriate personnel, whilst preserving its integrity at all stages.

The policy of information security is designed to prevent and minimise the impact of security incidents, ensure business continuity and minimise damage to the company, its clients, external providers and staff.

It is the policy of the company to ensure that:

- Information will be protected against unauthorised access
- Confidentiality, integrity and available of all information is preserved
- Regulatory, legislative and contractual requirements will be met
- Information security training will be provided
- Objectives are implemented and communicated
- All breaches of information security (actual or suspected) will be reported and investigated
- Standards will be produced to support this policy (including virus controls and passwords)
- Business requirements for the availability of information and information systems will be met
- Information required for a specific task is stored for a defined period

Data Protection Act 2018

The Company is fully committed to compliance with the requirements of the Data Protection Act 2018 and all other data protection legislation currently in force. The Regulation applies to anyone processing personal data and sets out principles which should be followed and gives rights to those whose data is being processed.

To this end, the Company endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- processed lawfully, fairly and in a transparent way (‘lawfulness, fairness and transparency’);
- processed no further than the legitimate purposes for which that data was collected (‘purpose limitation’);
- limited to what is necessary in relation to the purpose (‘data minimisation’);
- accurate and kept up to date (‘accuracy’);
- kept in a form which permits identification of the data subject for no longer than is necessary (‘storage limitation’);
- processed in a manner that ensures security of that personal data (‘integrity and confidentiality’);
- processed by a controller who can demonstrate compliance with the principles (‘accountability’).

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Company will:

- observe fully the conditions regarding having a lawful basis to process personal information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements;
- ensure the information held is accurate and up to date;
- ensure that the information is held for no longer than is necessary;
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018 (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information);
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection.

Employees' Personal Information

Throughout employment and for as long as is necessary after the termination of employment, the Company will need to process data about employees. The kind of data that the Company will process includes:

- any references obtained during recruitment;
- details of terms of employment;
- payroll details;
- tax and national insurance information;
- details of job duties;
- details of health and sickness absence records;
- details of holiday records;
- information about performance;
- details of any disciplinary and grievance investigations and proceedings;
- training records;
- contact names and addresses;
- correspondence with the Company and other information that you have given the Company.

The Company believes that those records used are consistent with the employment relationship between the Company and employees and with the data protection principles. The data the Company holds will be for management and administrative use only but the Company may, from time to time, need to disclose some data it holds about employees to relevant third parties, for example where legally obliged to do so by HM Revenue & Customs, where requested to do so for the purpose of giving a reference or in relation to maintenance support, and/or the hosting of data in relation to the provision of insurance.

In some cases the Company may hold sensitive data, which is defined by the legislation as special categories of personal data. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the Company's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, employees will be asked to give express consent for this information to be processed, unless the Company has a specific legal requirement to process such data.

Data Security

Employees are responsible for ensuring that any personal data held and processed as part of their job role is stored securely and not disclosed by any other means, accidentally or otherwise, to any unauthorised third party.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

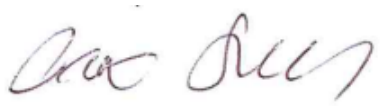
In the event that the company become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by a Director.

We will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

We will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

Record of Breaches

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under the Data Protection Act 2018. It records the facts relating to the breach, its effects and the remedial action taken.



Signed by Max Smith
Managing Director
August 2024