

## Data Protection Policy

### Introduction

The Company is required to maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations. The Company recognises the importance of the correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations.

The types of personal data that the Company may require includes information about: current, past and prospective employees; Company members; suppliers and others with whom it communicates. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

The Company fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for the Company must adhere to these principles.

### Principles

#### The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Be adequate, relevant and not excessive for those purposes;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purpose;
6. Be processed in accordance with the data subject's rights;
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;
8. And not be transferred to a country or territory outside 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.

## **Satisfaction of principles**

### **In order to meet the requirements of the principles, the Company will:**

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;
- take the appropriate technical and organisational security measures to safeguard personal data;
- and ensure that personal data is not transferred abroad without suitable safeguards.

## **The Company's Designated Data Controller**

The Company's Information Compliance Manager is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Managing Director. The Information Compliance Manager is James Hinton. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Information Compliance Manager.

## **Status of the Policy**

This policy has been approved by the Directors and any breach will be taken seriously and may result in formal action.

Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their Line Manager or the Company's Information Compliance Manager in the first instance.

## **Subject Access**

All individuals who are the subject of personal data held by the Company are entitled to:

- Ask what information the Company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the Company is doing to comply with its obligations under the 1998 Data Protection Act.

## **Employee Responsibilities**

All employees are responsible for:

- Checking that any personal data that they provide to the Company is accurate and up to date.
- Informing the Company of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the Company may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, employees collect information about other people (e.g. about personal circumstances, or about employees in the company), they must comply with the Policy and with the Data Protection Procedures which are contained in the Data Protection Manual.

## **Data Security**

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

## **Rights to Access Information**

Employees and other subjects of personal data held by the Company have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to the Company's Information Compliance Manager.

The Company reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request.

The Company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of a written request, unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

### **Publication of Company Information**

Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on staff contained within externally circulated publications such as the Company diary. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Company's Information Compliance Manager.

### **Subject Consent**

The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate Company policies, such as health and safety and equal opportunities.

### **Retention of Data**

The Company will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary.