Data Protection Policy

Policy Overview

In the course of your work, you may come into contact with and use confidential personal information about other employees, clients, customers, suppliers, agents, contractors and other people, such as their names and home addresses. This Policy helps you to ensure that you do not breach the Data Protection Act 1998. The Act provides strict rules governing the collection, retention, storage, use and disclosure of personal information. Information protected by the Act includes not only personal data held on computer but also certain manual records that form part of a structured filing system. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from your Manager. It is a criminal offence to knowingly or recklessly disclose personal data in breach of the Act. Accessing another Employee's personal records without authority is a disciplinary offence and may amount to potential gross misconduct.

The Company holds personal data about you and will process this data in accordance with your rights under the Act.

The Company's notification number is: Z6560541.

Data Protection Principles

The Act requires that eight data protection principles be followed in the handling of personal data. These are that personal data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes and not in any manner incompatible with those purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in accordance with the data subject's rights
7. Secure
8. Not transferred between countries without adequate protection

The Company is committed to following these principles and will be open and transparent about what the data will be used for. The Company will process personal data about you only as far as is necessary for the purpose of managing the Company's business in which you are employed. Unless you expressly authorise its disclosure, your personal data will not be disclosed to anyone else other than authorised Employees, those who provide relevant products to the Company (such as advisers and payroll administrators), regulatory authorities, potential or future employers, governmental or quasi-governmental organisations and potential purchasers of the Company or of that part of the business in which you work. The Company will only obtain personal data about you that it requires for the purpose of managing its business and dealing with you as an Employee of that business.

The Company will take all reasonable steps to ensure that the personal data it processes is accurate and not excessive. Personal data will be retained as necessary during the course of your employment and records will be retained for up to six years after you leave the Company's employment in case legal proceedings arise during that period. Different categories of data may be retained for different periods of time depending on legal, operational and financial requirements.

Data will only be retained for a period of longer than six years if it is material to ongoing legal proceedings or it should otherwise be retained in the interests of the Company after that period.

Manual personal data, such as personnel files, is stored in locked filing cabinets. Personal data held on computer is stored confidentially by means of password protection. The Company has network back-up procedures to ensure that data on computer cannot accidentally be lost or destroyed.

The Act prohibits the transfer of personal data outside the European Economic Area to countries that do not have similar protection of data except in some circumstances or with the subject's consent. The Company requires your consent under your Contract of Employment to such transfers should they be necessary. The reason for this is that, with the use of the Internet and email, data can be transferred to a computer or server in such a country in the course of a transfer between parties within the European Economic Area. Also the Company may have offices or subsidiary companies or agents or contractors in such countries now or in the future and therefore transfers of data could be necessary as part of the management of the Company's business and the performance of your Contract of Employment.

Consent to Processing

It is a requirement under the Act that you consent to the Company processing personal data about you. Some data is referred to in the Act as 'sensitive' personal data. This means personal data comprising information relating to:

- Race or ethnic origin
- Political opinions
- Trade Union membership
- Religious or other beliefs
- Physical or mental health or condition
- Sexual life
- Criminal offences both committed and alleged

It therefore follows that some of the personal information that the Company will have to process about you will be sensitive personal data, for example, information about your physical or mental health in order to monitor Sick Leave and take decisions about your fitness for work and your racial or ethnic origin, or religious or similar beliefs, in order to monitor compliance with equal opportunities legislation.

It is a term of your Contract of Employment that you expressly consent to the Company collecting, retaining and processing data including sensitive personal data about you for legal, personnel, administrative and management purposes. This data includes but is not limited to your name and address, salary details, bank details, date of birth, age, sex, ethnic origin, next of kin, sickness records, medical reports and details of criminal convictions. This information will only be used in order that we can monitor our compliance with the law and best practice in areas such as equal opportunity, pay and benefits, administration, performance appraisal and disciplinary matters. If your personal information changes, you should let us know so that our records can be updated.

Unless you give this consent it is not necessarily lawful for the Company to process the personal data that it needs in order to keep the necessary records about your employment and therefore it is not possible for the Company to meet the needs of running its business in relation to your employment without your consent.

Your Rights to Access Personal Information

Under the Act, you have the right to find out what personal information the Company holds about you, and to ask for a copy of that personal data. You also have the right to demand that any inaccurate data be corrected or removed and to seek compensation where you suffer damage or distress as a result of any breach of the Act by the Company.

You have the right on request to:

- Be told by the Company whether and for what purpose personal data about you is being processed.
- Be given a description of the personal data concerned and the recipients to whom it is or may be disclosed.
- Have communicated in an intelligible form the personal data concerned, and any information available to the Company as to the source of the data.
- Be informed in certain circumstances of the logic involved in computerised decision-making.

A request for access to any personal data that relates to you should be made in writing to your Manager and should specify what personal data your request relates to. The Company reserves the right to charge a fee of up to £10.00 or such higher amount as permitted by law from time to time before access can be granted. The Company also reserves the right to make further enquiries of you in order to satisfy ourselves as to your identity and to help us locate the personal data that you have requested.

Upon receipt of a request it is the Company's policy to provide copies of all personal data that the Company is obliged to disclose within 40 days of your request being received. The Company considers that if a period of less than one year has elapsed since any previous request for access to your personal data was complied with by the Company, it is not reasonable to expect the Company to be obliged to comply with a further request unless there are exceptional circumstances.

Should you wish to bring any inaccuracy in disclosed data to the attention of the Company you must do so in writing to your Manager. It is the Company's policy to ensure that all data is as accurate as possible and all necessary steps will be taken to ensure that this is the case and to rectify any inaccuracies.

Where the Company has requested a reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not to be disclosed to you, it is the Company's policy that it would normally be unreasonable to disclose such a reference to you unless the consent of the person who gave the reference is first obtained.

The Company reserves the right not to disclose to you any management forecasts or management planning documentation, including documents setting out the Company's plans for your future development and progress.

Your Obligations in Relation to Personal Information

You must comply with the following guidelines at all times:

- Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always

verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.

- Only transmit personal information between locations by fax or email if a secure network is in place, for example, a confidential fax machine or encryption is used for email.
- If you receive a request for personal information about another Employee, you should forward this to your Manager.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected.
- Do not include personal data in any email addressed to a recipient outside the European Economic Area without their prior explicit consent. Note: the EEA comprises Member States of the European Union plus Iceland, Liechtenstein and Norway.

If your personal circumstances change in any way, such as change of address, next-of-kin, etc., you should inform your Manager.