DATA PROTECTION POLICY

Introduction

In the course of your work you may come into contact with or use confidential information about employees, clients, customers and suppliers, for example their names and home addresses. The Data Protection Act 2018 contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of this policy is to ensure you do not breach the Act. 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 the Company's Data Protection Officer (see below). You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

This policy does not form part of an employee's contract of employment but it is a condition of employment that employees abide by this policy and therefore any failure to follow it can result in disciplinary proceedings.

The data protection principles

There are eight data protection principles that are central to the Act. The Company and all employees must comply with these principles at all times in their information-handling practices. In brief, the principles say that personal data must be:

1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given his consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

    - Race or ethnic origin.
    - Political opinions and trade union membership.
    - Religious or other beliefs.
    - Physical or mental health or condition.
    - Sexual life.
    - Criminal offences, both committed and alleged.

2. Obtained only for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes.

3. Adequate, relevant and not excessive in relation to the purposes for which it is processed. The Company will review employees' personnel files on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there is a sound business reason requiring information to continue to be held.

4. Accurate and, where necessary, kept up-to-date. If your personal information changes, for example you change address or you get married and change your surname, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company cannot be responsible for any such errors unless the employee has notified the Company of the relevant change.

5. Not kept for longer than is necessary. The Company will keep personnel files for no longer than six years after an employee has left the Company's employment. Different categories of data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a particular period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

6. Processed in accordance with the rights of employees under the Act.

7. Secure. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored as such in locked filing cabinets. Only authorised employees have access to these files. For a list of authorised employees, please contact Dr Adnan Niazi, the Company's Data Protection Officer. Files will not be removed from their normal place of storage without good reason. Data stored on diskettes or other removable storage media is kept in locked filing cabinets. Data held on computer is also stored confidentially by means of password protection, encryption or coding and again only the above employees have access to that data. The Company has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection relation to the processing of personal data.

Employees' consent to personal information being held

The Company holds personal data about its employees and, by signing your contract of employment, you have consented to that data about you being processed by the Company. Agreement to the Company processing your personal data is a condition of your employment.

The Company also holds limited sensitive personal data about its employees and, by signing this policy, you give your explicit consent to our holding and processing that data, for example sickness absence records, particular health needs and equal opportunities monitoring data.

Employees' rights to access personal information

Under the Act, employees have the right on request to receive a copy of the personal data that the Company holds about them, including personal data held on personnel files that form part of a relevant filing system, and to demand that any inaccurate data held be corrected or removed. They also have the right to seek compensation where damage and distress have been caused to them as a result of any breach of the Act by the Company.

Employees have the right, on request:

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

Upon request, the Company will provide you with a statement regarding the personal data held about you. This will state all the types of personal data the Company holds and processes about you and the reasons for which they are processed.

If you wish to access a copy of any personal data being held about you, you must make a written request for this and the Company reserves the right to charge you a fee of £10.00 for the supply of the information requested. If you wish to make a request, please complete a Personal Data Request Form, which can be obtained from the Data Protection Officer. Once completed, it should be returned to the Data Protection Officer. The Company will respond promptly and in any case within 40 calendar days of receiving the request. Note that the Company will always check the identity of the employee making the request before processing it.

If you wish to make a complaint that this policy has not been followed in respect of personal data the Company holds about you, you should raise the matter with the Data Protection Officer. If the matter is not resolved, it should be raised as a formal grievance under the Company's grievance procedure.

Exemptions

There are a number of exemptions from the data protection regime set out in the Act, for example:

- Confidential references that are given, but not those received by the Company from third parties. Only designated line managers can give Company references. Confidential references will not be provided unless the Company is sure this is the employee's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Employees' obligations in relation to personal information

You should ensure you 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 e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- If you receive a request for personal information about another employee, you should forward this to the Data Protection Officer, who will be responsible for dealing with such requests.
- 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.

Compliance with the Act is the responsibility of all employees. Any questions or concerns about the interpretation of this policy should be taken up with the Data Protection Officer.

Signed Dr Adnan Niazi

Issue Date 1/1/20
Last Reviewed On 03/07/26

Version 2