



1. Introduction

- 1.1. In the course of the use of the System you may come into contact with or use confidential information about persons appearing on the system (for example their names and home addresses). The Data Protection Act 1998 contains principles affecting the handling of personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data. 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 your Company's Data Protection Officer. You should be aware that you can be criminally liable if you knowingly or recklessly disclose personal data in breach of the Act.

2. The data protection principles

- 2.1. There are eight data protection principles that are central to the Act. The Company and all Users must comply with these principles at all times in their information-handling practices. In brief, the principles say that personal data must be:
- 2.1.1. 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 person 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.
- 2.1.2. Obtained only for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes.
- 2.1.3. Adequate, relevant and not excessive in relation to the purposes for which it is processed. Users must review personal data stored on the System on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there is a sound business reason requiring information to continue to be held.

- 2.1.4. Accurate and, where necessary, kept up-to-date. If personal information changes, for the Users must as soon as practicable update the relevant entries on the System.
- 2.1.5. Not kept for longer than is necessary.
- 2.1.6. Processed in accordance with the rights of data subject under the Act.
- 2.1.7. 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. Paper files containing confidential information should be stored locked filing cabinets. Only authorised persons should have access to these files. For a list of authorised employees, please contact your Company's Data Protection Officer. Files should not be removed from their normal place of storage without good reason. Data stored on memory sticks, discs or other removable storage media should be 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 persons have access to that data. Network back-up procedures are used to ensure that data on computer cannot be accidentally lost or destroyed.
- 2.1.8. 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.

3. Data Subject's rights to access personal information

- 3.1. Under the Act, data subjects have the right on request to receive a copy of the personal data that the System holds about them, 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.
- 3.2. Data subjects 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.
- 3.3. If a data subject wish to access a copy of any personal data being held about them, a written request must be made for this and the Company reserves the right to charge a fee of £10.00 for the supply of the information requested. If data subjects wish to make a request, they must complete a Personal Data Request Form, which can be obtained from your Company's Data Protection Officer. Once completed, it should be returned to your Company's Data Protection Officer. The Company will respond promptly. Note that the Company will always check the identity of the data subject making the request before processing it.

4. Exemptions

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

5. User's obligations in relation to personal information

- 5.1. You should ensure you comply with the following guidelines at all times:
- 5.1.1. 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.
 - 5.1.2. 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.
 - 5.1.3. 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.
 - 5.1.4. 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.
- 5.2. Compliance with the Act is the responsibility of all Users. Any questions or concerns about the interpretation of this policy should be taken up with your Company's Data Protection Officer.