# Data Protection Policy

Revised: May 2018
Next review: May 2019

**The data protection principles**

During your work, you may come into contact with, or use confidential information about employees, clients and customers, for example their names and home addresses. The Data Protection Act 1998 (the Act) 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 these rules is to ensure that 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 Paul Stephens (Data Protection Officer).

You should be aware that, under the Act, you are personally accountable for your actions and you can be held criminally liable. It is a criminal offence under s.55 of the Act for you knowingly or recklessly to obtain or disclose personal data (or to procure its disclosure to a third party) without the consent of the data controller. This would include, for example, taking clients' or customers' contact details or other personal data without the Company's consent on the termination of your employment, accessing another employee's personnel records without authority or otherwise misusing or stealing personal data held by the Company.

It is also an offence to sell, or to offer to sell, personal data if it has been obtained in contravention of s.55. Where unlawful activity is suspected, the Company will report the matter to the Information Commissioner's Office for investigation into the alleged breach of the Act and this may result in criminal proceedings being instigated against you. You may have to pay an unlimited fine and a victim surcharge if you are found guilty of the criminal offence. The Company may also need to report the alleged breach to a regulatory organisation or body.

Any serious breach of data protection legislation will also be regarded as misconduct and will be dealt with under the Company's disciplinary procedures. If you access another employee's personnel records without authority, or you otherwise unlawfully obtain or disclose personal data (or procure its disclosure to a third party) without the Company's consent, this constitutes a gross misconduct offence and could lead to your summary dismissal.

There are eight data protection principles that are central to the Act. The Company and all its employees must comply with these principles at all times in its 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 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 not processed in a manner incompatible with those purposes.

3. Adequate, relevant and not excessive. The Company will review personnel files on an annual basis to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.

4. Accurate and kept up to date. If your personal information changes, for example you change address, you must inform your line manager as soon as practicable so that the Company's records can be updated. The Company cannot be held responsible for any errors unless you have 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 termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data which the Company decides it does not need to hold for a period of time will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a maximum period of one year.

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

7. Processed so as to ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personnel files are confidential and are stored in locked filing cabinets. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on discs, memory sticks, portable hard drives or other removable storage media will be kept in locked filing cabinets or locked drawers when not in use by authorised employees. Data held on computer will be stored confidentially by means of password protection, encryption or coding, and again only authorised employees have access to that data. The Company has network backup 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 ensures an adequate level of protection for the processing of personal data.

**Your consent to personal information being held**
The Company holds personal data about you. By signing your contract of employment, you have consented to that data being processed by the Company for any purpose related to your

continuing employment or its termination including, but not limited to, payroll, human resources and business continuity planning purposes. Agreement to the Company processing your personal data is a condition of your employment. This includes giving your consent to the Company using your name, photograph and a brief work experience history in its marketing or promotional material, whether in hard copy print format or online on the Company's website. It also includes supplying the Company with any personal data that it may request from you from time to time as necessary for the performance of your contract of employment or the conduct of the Company's business, for example, supplying up-to-date contact telephone numbers to be held by line managers as part of its business continuity plan.

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

**Your right to access personal information**
You have the right, on request, to receive a copy of the personal information that the Company holds about you, including your personnel file, and to demand that any inaccurate data be corrected or removed. You also 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 data and the recipients to whom it may be disclosed
- have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data
- be informed 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. It 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 up to £10. To make a request, please complete a Personal Data Subject Access Request Form, which can be obtained from the Data Protection Officer.

If you wish to make a complaint that these rules are not being 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 to your satisfaction, it should be raised as a formal grievance under the Company's grievance procedure.

**Your obligations in relation to personal information**
If, as part of your job duties and responsibilities, you collect personal information about employees or other people such as clients or customers, you must comply with this policy. This includes

ensuring the information is processed in accordance with the Act, is only processed for the purposes for which it is held, is kept secure and is not kept for longer than necessary. You must also comply with the following guidelines at all times:

- do not disclose confidential personal information to anyone except the data subject. In particular, it should not be:

1. given to someone from the same family
2. passed to any other unauthorised third party
3. placed on the Company's website
4. posted on the Internet in any form

unless the data subject has given their explicit prior written 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
- where the Company provides you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the Company's requirements in this regard
- 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 is responsible for dealing with such requests
- ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons
- do not access another employee's personnel records without authority as this will be treated as gross misconduct and it is a criminal offence under the Act
- do not obtain or disclose personal data (or procure its disclosure to a third party) without authority or without the Company's consent as this will be treated as gross misconduct and it is a criminal offence under the Act
- do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject
- do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager
- ensure that, when working on personal information as part of your job duties when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the Act, in particular in matters of data security
- ensure that hard copy personal information is disposed of securely, for example cross-shredded
- ***remember that compliance with the Act is your personal responsibility. If you have any questions or concerns about the interpretation of these rules, please contact the Data Protection Officer.***