
Data Protection Policy

Purpose

To set out the Company's policy and procedures to meet the requirements of the Data Protection Act 1998 ('DPA'). It should be made immediately available to employees and other individuals upon request.

Scope

This policy applies to all employees of the Company, casual workers, agency staff and contract workers. This policy does not form part of any employee's contract of employment and may be amended at any time.

Principles

The Data Protection Act 1998 ("DPA") gives rights to individuals, about whom personal data is obtained or processed, whether manually (in certain paper-based filing systems) or automatically (i.e. processed by a computer). The DPA places obligations on organisations which hold and/or process data about any such individuals. "*Personal data*" is data that which identifies a living individual.

Processing of data

It is the responsibility of every employee to ensure their familiarity with this policy and to comply with it. Any breach of this policy may result in disciplinary action (up to and including dismissal) and may constitute a criminal offence. Employees should report any breach of this policy to Human Resources.

Purpose and method of data collection

The purpose of data collection is designed specially to provide:

- Information, whenever required, for planning and managing the Company's organisational structure
- Information, whenever required, for dealing with customers' enquiries
- Individual information for managing the employment, deployment and welfare of individual employees
- Information, whenever required for responding to legitimate external enquiries about the Company's employees and/or customers, and
- Assistance with personnel and salary administration procedures, e.g. payroll

Disclosure of data

To ensure compliance with the DPA and in the interests of privacy, and good relations, disclosure and usage of information held by the Company is governed by the following conditions:

- It will be used only for one or more of the purposes specified in this policy
- Provided that the identification of individuals is not disclosed, statistical information may be used to respond to any legitimate internal or external requests for data
- Personal data must not be disclosed to any unauthorised recipient

Authorised requests for data by external recipients of data are:

- Requests by the individual who is the subject of the data, for e.g. mortgage request, references and bank mandates
- Requests made for the purposes of law enforcement (i.e. for the prevention or detection of crime, the assessment or collection of any tax or duty or the assessment or collection of any liability via the Child Support Agency)
- Requests in relation to any other legal processes
- Requests, if urgently required, for the prevention of injury and damage to health
- Requests required by specifically identified external sources, e.g. pension administrators, in order to administer the Company's participation in various external pension schemes

Monitoring

Please note that the Company may at any time and without notice monitor or keep a record of communications sent and received over its IT resources (including: computer hardware and software, telephone, fax machines, voicemail, e-mail, building and facility access and CCTV systems) and/or record your use of the Company's IT resources in order to:

- Detect and/or prevent crime
- Establish the existence of business related facts
- Ascertain whether you are complying with the Company's rules and policies and any statutory and/or regulatory requirements to which either you and/or the Company are subject
- Ascertain whether you are attaining requisite standards of service
- Carry out maintenance of IT resources and monitor for viruses
- Investigate or detect unauthorised use of the Company's IT resources
- Protect your individual interests

Data Protection Policy

The Company may use CCTV monitoring on its premises to:

- Protect your personal safety and the safety of the public when they are on the Company's premises
- Investigate detect and/or prevent crime and to apprehend/prosecute offenders, and/or
- Ascertain whether you are complying with behavioural requirements and achieving the standards set in your employment contract, the Company's rules and policies and any applicable statutory and/or regulatory obligations to which you are subject.

Any such CCTV monitoring will be carried out in accordance with the principles established in the Data Protection Act.

The Company may sometimes disclose CCTV footage to third parties, such as law enforcement authorities and the Courts for the purposes listed above, but any such disclosure will take place in accordance with the principles established in the Data Protection Act.

Accuracy of data

Data shall be updated where necessary to ensure it remains accurate.

Employees' rights

Employees are, at reasonable intervals entitled to have access to personal data held upon them which is not excluded data (see paragraph below).

The Company will comply with a request from any other individual to supply a record of their personal data within 40 days of the date on which the request is made accompanied by the prescribed fee (currently £10). Requests should be put in writing to Human Resources. Any member of staff who receives a written request should forward it to Human Resources immediately.

The following information is excluded from the above:

- Confidential references given by the Company relating to training, employment or providing a service.
- Personal data processed for the purposes of management forecasting to the extent that disclosure would be likely to prejudice the conduct of that business or activity only.
- Personal data which consists of records of the intentions of the Company relating to any negotiations with the individual to the extent that disclosure would be likely to prejudice those negotiations only.
- If, in order to comply with a disclosure request, the Company would need to disclose information relating to an identifiable third party then disclosure is not required unless the third party consents or it is otherwise reasonable to comply with the request without such third party consent.

In addition to seeking disclosure of information, an individual is also entitled to request that the Company does not process data concerning him/her where this will cause or be likely to cause substantial and unwarranted damage or distress to the individual concerned or to a third party.

An employee who feels that he/she has, or is likely to suffer damage as a result of either inaccuracy in the data held by the Company or as a result of unauthorised disclosure of information must notify Human Resources in writing immediately. Where appropriate, the Company will correct or erase that information.

Security

Access to personal data is restricted to Human Resources, Accounts and where applicable, managers. Individuals seeking access to personal data must notify one of those departments.

All personal data will be stored in such a way that access is only permitted by authorised personnel and any disposal of that information will also be conducted in a secure way.

Third parties

Any personal data which the Company receives and processes in relation to third parties, will be obtained lawfully and fairly and dealt with in accordance with the principles and conditions of the Act.

Personal data will only be transferred, for purposes connected with your employment, to a third-party data processor if he agrees to comply with our procedures and policies for keeping personal data secure, or if he puts in adequate measures himself.

Revision of the policy

It is important to note that the Company may vary or amend this policy from time to time particularly to take account of changes in the law, best practice or business requirements. This document shall be revised by the appropriate person, the HR Manager or nominated deputy. You will be notified of any changes.