

# Data Protection Policy 2025



## Background & Objectives of the Policy

The Company collects, stores, and processes personal information about people (e.g. employees, workers, contractors, customers, etc) and recognises the need to treat it in an appropriate and lawful manner.

This policy aims to inform individuals about how their information is processed and of their rights of access to information held about them.

This policy applies to all employees, workers and contractors and helps ensure that we do not breach the Data Protection Act 2018, which provides rules in this area.

The Data Protection Act 2018 (DPA) safeguards individuals against the misuse of their 'personal data' by regulating the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

The Data Protection Act 2018 requires that the following data protection principles be followed in the handling of personal data. These are that personal data must:

- be fairly and lawfully processed.
- be processed for limited purposes and not in any manner incompatible with those purposes.
- be adequate, relevant, and not excessive.
- be accurate.
- not be kept for longer than is necessary.
- be processed in accordance with individuals' rights.
- be secure; and
- not be transferred to countries without adequate protection.

The policies adopted by the Company endeavour to ensure that these data protection principles are adhered to.

## Policy Details

### Personal Data

'Personal data' means any information relating to a living individual who can be identified from that data and includes any expression of opinion about the individual and any indication of the intentions in respect of the individual.

It is necessary for the Company to hold certain personal data relating to our employees in order to operate our business and fulfil our legal obligations.

Personal data on existing and past members of staff is held securely on the Human Resources database and on an employee's Personal file. These can only be viewed by the HR Department. In the rare event that manual records are removed from the Human Resources Department they will be checked out formally and must be kept securely. This will only be at the discretion of the Human Resources Manager.

# Data Protection Policy 2025



The following list (which is not exhaustive) gives examples of data that are held on manual or computer records within the Company:

- Personal details: date of birth, address, marital status, bank account, etc.
- Recruitment records: Application forms, CVs, new starter details and references
- Training records, Performance and Development reviews (PDR)
- Career details: salary increases, benefits and promotions.
- Attendance: timekeeping, and absence
- Disciplinary records: disciplinary actions and under performance warnings and supporting documentation.
- Monitoring: usage of e-mail, internet, and telephone systems
- Surveillance: CCTV and photographs.

## **Sensitive Personal Data (including customer and third-party data if relevant)**

This includes:

- Diversity information relating to ethnic origin, religion, and sexual orientation.
- Trade union membership, if applicable.
- Medical reports and/or fit notes relating to health or disability.
- Offences or alleged offences, criminal proceedings, or their outcome.

The Company shall endeavour to notify employees when such information is collected and ensure that it is used only for the purposes that have been notified. In most cases, the individual's consent will be required to the processing of sensitive personal data.

## **Locally Held Records**

Records may be kept outside the HR department in the company in regional / divisional offices, for example, file notes, PDRs or CVs (which may be used for purposes of tendering and / or marketing). The holder will be personally responsible for ensuring that all data held on employees locally, are kept only when it is absolutely necessary. The holder is also responsible for ensuring that remotely held records fully comply with the Data Protection Act, and in particular that they are well maintained, up to date and held securely.

All other records must be forwarded to Human Resources (including all formal written correspondence with the employee, self-certification forms and medical certificates), to ensure confidential and up to date record keeping.

## **Disclosing Personal Data**

Where personal data is disclosed to third parties, it will be restricted to only those details that are required for the job in hand. The Company may make the following disclosure of personal data about employees:

# Data Protection Policy 2025



- Within the Company: Personal data will be disclosed or transferred only as authorised by the Company to other companies within the Group (known as Associated Companies) or companies in whom the Company or Associated Company has a shareholding.
- Third Parties: providers that administer pay and benefits also need to access and process personal data.

Apart from the above no personal data will be offered to an external source, without the express agreement from the employee (e.g. mortgage references) unless the Company is legally obliged to.

## Ensuring accuracy

It is important that the personal data that is held by the Company is kept up to date. Should any information supplied by an employee become inaccurate, such as a change of address, the employee should let the Company know so that the HR records can be updated.

## Security

Data processors (any individuals who have access to and process employee computerised or manual records) must exercise caution in responding to external requests for any information on current or ex employees' personal details. They should be aware that such individuals may be using deception to gain access to information that they are not entitled to. It is therefore important to establish the identity of the person you are speaking to and where practicable obtain the request in writing. For telephone requests for information, a telephone number should be taken so that they can be called back to verify they are who they say they are.

It is Company policy that verbal references will not be given or requested.

## E-mails

E-mails are also covered by the Data Protection Act. By sending E-mails you are consenting to the processing of any personal data contained in that E-mail and are explicitly consenting to the processing of any sensitive personal data contained in that E-mail. If you do not wish the Company to process such data, you should communicate it by other means.

When sending E-mails containing personal information relating to other people you must ensure that you are authorised to release this information to the recipient. The explicit permission of the employee may be required for certain sensitive data. If in doubt, speak to the Human Resources Department. The unauthorised release of information may lead to a breach of the Data Protection Act and could lead to disciplinary action and possible prosecution.

# Data Protection Policy 2025



## CCTV

Visual and other methods of surveillance, such as CCTV and photographs, will only be used for the following purposes:

- Detecting and observing intruders
- Granting access to restricted areas
- Tracking visitors who may pose a security threat.
- Reducing pilferage, delinquent behaviour, and sabotage
- Countering fraud and the misuse of company resources
- Dealing with suspected harassment
- Providing evidence for use before the courts

The Company reserves the right to refer to any recordings where CCTV may assist in respect of disciplinary proceedings.

## Sale or transfer of business

If the Company sells all or part of its business, it may provide personal data about you to any prospective purchaser in the course of negotiations. So far as possible such data will be provided in an anonymous form and if this is not possible the prospective purchaser will be required to keep the information confidential. We will transfer your personal data on any transfer or sale falling within the terms of the Transfer of Undertakings (Protection of Employment) Regulations 2006.

## Request for access to personal data

In accordance with the provisions of the DPA, employees have certain rights to request access to their own personal data. To make such a request please do so in writing to the HR Department.

Signed:  Group Director

Date : 20/03/2025