Data Protection Policy

Purpose

The Company is committed to being transparent about how it collects and handles the personal information of its employees, and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, as well as employee rights and obligations in relation to data protection and any relevant Data (please see definition below).

Employees must read, understand and comply with this policy when Processing Data on the Company's behalf. This policy sets out what we expect from you in order for the Company to comply with the applicable law.

For the purposes of this policy only, 'employees' shall refer to all staff including, employees, workers, self-employed contractors and any other staff who the Company Processes Data in relation to.

Definitions to help you understand this policy

- "Data" means personal data and special categories of personal data, unless specified otherwise.
- "Personal Data" is any information that relates to employees who can either be directly identified from that information or indirectly identified if that information was connected with other information.
- "Processing" is any use that is made of data, including collecting, storing, amending, disclosing or destroying it (also includes 'processes' and 'process').
- "Special Categories of Personal Data" means personal data revealing an employee's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data.
- "Criminal Records Data" means information about an employee's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The Company processes HR-related data in accordance with the following data protection principles.

The Company:
- Processes data lawfully, fairly and in a transparent manner;
- Collects data only for specified, explicit and legitimate purposes;
- Processes data only where it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Keeps accurate data and takes all reasonable steps to ensure that any inaccurate data is rectified or deleted without undue delay;
- Does not keep data in a form which permits identification of employees for longer than is necessary for the purposes for which data is processed;
- Does not transfer data to another country without appropriate safeguards in place;
- Permits employees to exercise certain rights in relation to their data, including rights of access where applicable; and

- Adopts appropriate measures to make sure that data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Transparency & Notice

The Company shall provide employees with an employee privacy notice which contains information relating its processing of employee data, including (but not limited to):

- The purposes for processing employee data;
- How it processes employee data;
- The relevant legal basis for such processing;
- Any relevant transfers of employee data; and
- Who to contact if employees have any concerns regarding the processing of their data.

The Company confirms that it will process data relating to employees in conformance with the employee privacy notice and with this policy.

The Company may Process Special Categories of Personal Data or Criminal Records Data in order to perform its legal obligations or to exercise its rights under employment law.

The Company will update HR-related data promptly if an employee advises that his/her information has changed or is inaccurate.

Some data collected and processed by the Company is held in the employee's personnel file (in hard copy or electronic format, or both), and on HR systems.

The periods for which the Company retains HR-related data are contained within its employee privacy notice or any relevant data retention policy/guidelines from time to time in force.

Employee rights

As a data subject, an employee has a number of rights in relation to the handling of their data:

Subject access requests
Employees have the right to make a subject access request. If an employee makes a subject access request, the Company will inform him/her:
- Whether or not his/her data is processed and if so why, the categories of data concerned and the source of the data if it is not collected from the employee;
- To whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area ('EEA') and the safeguards that apply to such transfers;
- For how long his/her data is stored (or how that period is decided);
- His/her rights to rectification or erasure of data, or to restrict or object to processing;
- His/her right to complain to the Information Commissioners Office ('ICO') if he/she thinks the Company has failed to comply with his/her data protection rights; and
- Whether or not the Company carries out automated decision-making and information about how such decisions are made, including the significance and consequences of the automated decision.
-

The Company will also provide the employee with a copy of the data undergoing processing. This will normally be in electronic form if the employee has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the employee should send the request to the HR department. In some cases, the Company may need to ask for proof of identification before the request can be processed. In such circumstances, the Company will inform the employee if it needs to verify his/her identity and the documents it requires to do so.

The Company will normally respond to a subject access request within a period of one month from the date it is received. In some cases, such as where the Company Processes large amounts of the employee's Data, it may respond within three months of the date the request is received. The Company will write to the employee within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond to the request but it will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an employee submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

Other rights

The Company shall process data in a way that enables employees to exercise their rights under applicable laws. Those rights are as follows:

- Transparency – the right to receive information about the Processing of their data;
- Access – the right to receive certain information relating to the Company's use of your Data (as outlined above);
- Rectification – the right to rectify or update any inaccurate data;
- Erasure – the right to request erasure of Data in certain circumstances, for example where the Data is no longer necessary for the purposes of processing or where the employee's interests override the Company's legitimate grounds for processing that data (only where the Company relies on its legitimate interests as a reason for processing data);
- Objection/restriction – the right to object to processing of data in certain circumstances, for example where it is unlawful or inaccurate.
- Portability – the right to receive the data processed by the Company in certain circumstances, including where Processing is undertaken by automated means.
- Withdrawal of consent – the right to withdraw consent at any time where the Processing of Data is based on the employee's consent.
- Complaint – the right to lodge a complaint with the ICO.

In order to enforce any of these rights, the employee should send the request to the HR Department.

Data security

The Company takes the security of HR-related Data seriously.
The Company shall maintain adequate technical and organisational security measures designed to safeguard the Data of employees against unauthorized access or disclosure.

Where the Company engages third parties to process data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organizational measures to ensure the security of any data.

The Company will endeavour to design its systems and business processes which process data to minimise the risks to the privacy, rights and freedoms of employees. This may include carrying out Data Protection Impact Assessments where necessary and maintaining appropriate records of the Processing that the Company carries out.

Employee responsibilities

Employees are responsible for helping the Company keep their data up to date. Employees should inform the Company if the data it has provided to the Company has changed, for example if an employee moves house or changes his/her bank details.

Employees may have access to the data of other employees and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the Company relies on employees to help meet its data protection obligations to staff and to customers and clients.

Employees must immediately report the discovery of any actual or potential security incident and data breach (including unauthorised access or disclosure of employee's Data) to the HR Department. The Company has an obligation under law to report any data breach and employees are expected to assist the Company in complying with its legal reporting obligations. Failure to do so may constitute a disciplinary offence as outlined below.

Employees who have access to other employees' data are required:

- To access only data that they have authority to access and only for authorised purposes;
- Keep and maintain accurate corporate records reflecting our processing including records of consents from third parties, including customers and clients where relevant.
- Not to disclose data except to employees (whether inside or outside the Company) who have appropriate authorisation;
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove data, or devices containing data or that can be used to data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and/or the device; and
- Not to store data on local drives or on personal devices that are used for work purposes.
- Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing or disclosing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Amendments to Policy

Date	Person	Brief Outline	Approval Date	Approver
May 2023	Rachel Holmes	Policy Created	19 June 2023	James York