Data Protection Policy

Purpose
The Company is committed to being transparent about how it collects and uses the personal data of its employees, and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and employee rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees and former employees, referred to as HR-related personal data.

The Company has appointed Dr Katy Read, Executive Director, as the person with responsibility for data protection compliance within the Company. She can be contacted at katy.read@middlemarch-environmental.com. Questions about this policy, or requests for further information, should be directed to her.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Principles
The Company processes HR-related personal data in accordance with the following data protection principles:

- The Company processes personal data lawfully, fairly and in a transparent manner.
- The Company collects personal data only for specified, explicit and legitimate purposes.
- The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Company keeps personal data only for the period necessary for processing.
- The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company tells employees the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of employees for other reasons. Where the Company relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of employees.

Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a procedure on special categories of data and criminal records data.

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

Personal data gathered during employment is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to employees.

The Company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the Data Protection Act 2018.

Individual Rights
As a data subject, employees have a number of rights in relation to their personal data.

Subject Access Requests:
Employees have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- 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 personal 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 Commissioner 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 the logic involved in any such decision-making.

The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic format unless the employee specifies the way they want to access their data.

If the individual wants additional copies, the Company may charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the employee should use the Company's Subject Access Request Form FP-18. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the employee if it needs to verify his/her identity and the documents it requires.

The Company will normally respond to a 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 but 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
Employees have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the employee's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the employee's interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should complete the relevant Request Form (see Forms FP-19 To FP-21) and send the request to Dr Katy Read, Executive Director.

Data Security
The Company takes the security of HR-related personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. HR-related personal data pre-2018 is stored in paper format in locked cabinets with access available to the Managing Director and Office Manager only. Data from Jan 2018 onwards is held stored electronically on Citation's Atlas computer system. Access to the data stored on this system is restricted to Directors, HR-managers and the Office Manager.

Where the Company engages third parties to process personal 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 organisational measures to ensure the security of data.

Impact Assessments
Some of the processing that the Company carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for employees and the measures that can be put in place to mitigate those risks.

Data Breaches
If the Company discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of employees, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of employees, they will be informed that there has been a breach and provided with information about its likely consequences and the mitigation measures it has taken.

International Data Transfers
The Company will not transfer HR-related personal data to countries outside the EEA.

Employee Responsibilities
Employees are responsible for helping the Company keep their personal data up to date. Employees should let the Company know if data provided to the Company changes, for example if an employee moves house or changes his/her bank details.

Employees may have access to the personal data of other individuals and of our customers and clients in the course of their employment. 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 who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (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 personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to Dr Katy Read, Executive Director immediately.

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 employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training
Employees whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive training to help them understand their duties and how to comply with them.

Dr Philip Fermor
Managing Director

Approved at MEL Board on 19th December 2018
Next review date: December 2020