**Data Protection Policy**

As your employers, we hold certain personal information on you and all its employees. We only hold and retain personal data for as long as needed. This retention period is based on the business needs, the current and future value of the information; the costs, risks and liabilities associated with retaining the information; and the ease or difficulty of ensuring it remains accurate and up to date.

We have appointed [name and job title] as the Data Protection Officer (DPO) responsible for data protection compliance within the company. They can be contacted at [email address]. Questions about this policy, or requests for further information, should be directed to them.

Data is only collected for specific purposes and only used for these purposes. All forms of gathering information state their specific reason for collection. Personal information is kept in the personnel record, held securely within the business/on HRIS.

We will comply with all statutory requirements of the General Data Protection Regulation (GDPR) by registering all your personal data held on its computer and/or related electronic equipment and by taking all reasonable steps to ensure the accuracy and confidentiality of such information.

You have the following rights as defined by GDPR:

* to be informed
* to access
* to rectification
* of erasure
* to restrict processing
* to data portability
* to object

The GDPR protects your rights concerning information about you held on your computer. Anyone processing personal data must comply with the seven principles of good practice. Data must be:

* processed lawfully, fairly and with transparency
* processed for specified, explicit and limited purposes
* adequate, relevant, and limited to what is necessary for relation to the purposes for which it is processed
* accurate and kept up to date
* not kept longer than necessary
* processed in accordance with the data subject’s rights
* processed securely

**Requesting Access**

If you wish to request access to your personal data held by us, you should do so in writing by emailing the DPO, who will respond within one month. Please be aware that HR will conduct security checks to verify your identity to grant access. This service is only charged if the request is deemed excessive. Aligning with the right to portability, you can obtain personal data and move it or copy it securely and easily from one IT platform to another for personal purposes.

**Erasure**

You have the right to request the deletion of your personal data where there is no evidence for the need to continue processing it or where there is no justifiable basis for processing the data any longer. If you wish to exercise this right, please write your request to the email address detailed above. Please be aware that they will conduct security checks to verify your identity and grant your request.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

* to exercise the right of freedom of expression and information;
* to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
* for public health purposes in the public interest;
* archiving purposes in the public interest, scientific research, historical research, or statistical purposes;
* the exercise or defence of legal claims.

**Rectification**

If you deem any information to be inaccurate, you can either amend this information yourself if you are able or contact the DPO / HR, who will correct it within one month.

**Third Parties**

Where we engage with third parties, such as Breathing Space HR, to process personal data on our behalf, such parties do so based on written instructions, are under a duty of confidentiality, and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

**Reporting a Security Breach**

A personal data breach means a breach of security leading to the destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data. If you believe a breach has occurred, don't hesitate to contact the DPO so they can investigate. Any security breaches should be reported to the supervisory authority (ICO – Information Commissioners Office) immediately and within 72 hours. If the breach is of risk to an individual, they should also be informed. A breach notification should include the following:

* the nature of the personal data breach, including, where possible: the categories and an approximate number of individuals concerned; and the categories and an approximate number of personal data records concerned.
* the name and contact details of the DPO or other relevant contact point where more information can be obtained.
* a description of the likely consequences of the personal data breach; and
* a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

**Employee Responsibilities**

You are responsible for helping us keep your personal data up to date. Let us know if the data provided to you change, for example, your address or bank details.

You may have access to the personal data of other individuals in the course of your employment. Where this is the case, we rely on you to help meet its data protection obligations to all its employees.

If you have access to personal data, you are required to:

* to access only data that you have authority to access and only for authorised purposes;
* not to disclose data except to individuals (whether inside or outside the organisation) 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 information that can be used to access personal data from our premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
* not to store personal data on local drives or personal devices used for work purposes.

Failing to observe these requirements will be classed as misconduct, which will be dealt with under the Resolution procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason, may constitute gross misconduct and lead to dismissal without notice.

**Training**

We will train you regarding your data protection responsibilities during your induction and at regular intervals afterwards. If your role requires regular access to personal data, you will receive additional training to help you understand your duties and how to comply with them.