PRIVACY POLICY

Job Applicants, Current and Former Employees

1. Introduction

Flexible Respite (the Company) is committed to protecting the privacy and security of your personal data. This Privacy Policy describes how we collect and use your data during and after your employment with us. This may be supplemented by additional privacy notices in certain specific instances, which set out in further detail how and why we use your personal data.

2. Scope

This Policy applies to all Company employees; ie those employed on a Company contract of employment) including those on fixed-term and casual engagements. It does not apply to agency workers, consultants or self-employed contractors.

This Policy is not contractual and does not form part of an employee's terms and conditions of employment; and may be subject to change at the discretion of the Company.

The content of this Policy is not exhaustive. Instances may occur that fall outside of the areas covered in this document. The Company reserves the right, whilst acting fairly and reasonably, to take such measures as are necessary in each individual case.

3. Responsibilities

The Company **i**s the data controller for the information that we hold about you as a result of your employment with us. We decide how to use your data and we are responsible for managing your personal data.

The Company's Directors have overall responsibility for this Policy and have delegated the day to day responsibility for its operation to the HR Manager. Any queries or suggestions relating to this Policy should be addressed to the HR Manager and sent to admin@flexiblerespite.com

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

Individuals may have access to the personal data of other individuals [and of our Clients] in the course of their employment, the Company relies on individuals to help meet its data protection obligations to staff [and to Clients].

Individuals 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 the Company

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

The Company will provide training to all individuals about their data protection responsibilities as part of the induction process [and at regular intervals thereafter]. Individuals 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 additional training to help them understand their duties and how to comply with them.

4. What is Personal Data and Sensitive Personal Data?

Personal data is any information relating to an identified or identifiable individual and from which that individual can be directly or indirectly identified. It does not include information where your identity has been removed (anonymised information).

Sensitive personal data is information relating to an identified or identifiable individual that fall within special categories, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, sex life or sexual orientation.

5. What Personal Data do we collect about you?

The personal data that we expect to collect, hold and use about you is likely to include the following. This list is not exhaustive but is intended to give you a clear idea of the personal data about you which we process:

- Personal details such as name, title, addresses, telephone numbers, and personal email addresses, date of birth, gender, marital status and dependants, National Insurance number, copy of driving licence and / or other photographic ID such as a passport;
- Next of kin and emergency contact information;
- Bank account details, payroll records and tax status information;

- Salary, annual leave, pension and benefits information;
- Start date and termination date;
- Location of employment or workplace;
- Recruitment information (including copies of right to work documentation, references, interview notes and opinions taken during and following interviews and other information in a application form/ CV or cover letter as part of the application process) which may be electronic or physical copies;
- Employment records (including job titles, work history, working hours, training records, contracts and professional memberships, absence records including holiday records, self-certification forms and medical certificates);
- Details of your professional qualifications and education history;
- Compensation history;
- Performance information;
- Disciplinary, conduct and grievance information;
- Information about your use of our information, communication and technology systems;
- Information relating to expense claims;
- Photographs;
- Your vehicle registration number;
- Details of your working hours and attendance records;
- Details in references about you that we provide to others;
- Communications with those responsible for managing you and others working with you.

The above may include 'special categories' of more sensitive information such as:

- Information about your race, ethnicity, religious beliefs and sexual orientation. This personal data will only be processed where you have volunteered it and you need to process it in order to ensure meaningful equal opportunity monitoring and to meet our statutory obligations under the Equality Act 2010 and other relevant legislation;

- Trade union membership. This personal data will be used to pay trade union premiums, register the status of a protected employee and to comply with employment legislation;

- Information about your health, including any disability and/or medical condition, health and sickness records. This information will only be processed where it is necessary (for example to record absence from work due to sickness, to arrange to make appropriate payments for sick pay, to determine your fitness for work or to determine whether it is necessary to make reasonable adjustments for disability). Processing of this nature is necessary to carry out our obligations and/or exercise our rights as an employer, for the purposes of occupational health and for the assessment of the working capacity of employees. There may also be circumstances where we ask for your explicit consent to share data about your health;

- Biometric data. This information may be used as part of the recruitment process so as to comply with right to work checks and for the purpose of accessing electronic, communication and technology systems;

- Information about criminal convictions and offences, including proceedings or allegations. Data about spent criminal convictions or any barring decisions will only be collected for particular roles, where we are legally required to do so and where have told you that we are collecting this information. If a post requires additional screening you will be advised before the screening takes place. We may also process data relating to criminal conduct for disciplinary reasons in order to exercise rights under our contract with you.

We will only process sensitive personal data where absolutely necessary, specifically including in order to defend legal claims. We will ensure that any sensitive personal data is kept securely and only seen by those who have to see it.

The provision of information for us to monitor diversity is voluntary and will be anonymised as far as possible. You have the right to tell us to edit/delete personal data that you have provided to us and that you no longer wish us to process for the purpose of monitoring diversity.

We do not need your consent if we use special categories of your personal data in accordance with our written policy to carry out our legal obligations or exercise specific rights in accordance with employment legislation. For example, to ensure we provide you with a safe place of work or to consider making reasonable adjustments. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive personal data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. It is not a condition of your contract with us that you agree to any request for consent from us.

6. How will we process your Personal Data?

We obtain the vast majority of information directly from you through the application and recruitment process. We may also obtain information from third parties, such as employment agencies, background check providers or referees.

We will collect additional information about you during your contract with us. This will usually be directly from you, but may be from third parties such as medical practitioners, payroll/ pension administrators, insurance benefit administrators, your trade union, other employees, consultants and other professionals we may engage to advise the business, communication systems, remote access systems, telephones, voicemails, mobile phone record, tools to monitor use of communication systems and data-loss prevention tools.

We will comply with data protection law by taking steps to ensure that the information that we hold about you is:

- Used lawfully, fairly and in a transparent way;
- Only collected for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- Relevant to the purposes we have explained to you and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the purpose we have explained to you; and
- Kept securely.

7. How long will we process your information?

We will retain your personal data so long as it is necessary to fulfil the purposes we collected it for, including satisfying any legal, accounting or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure

of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the Company we will retain and securely destroy your personal data in accordance with our Data Retention Policy.

8. Reasons and Purpose for processing your personal data

We are clear on the purpose for which we collect your personal data and rely on a number of lawful reasons for processing your personal data arising out of your relationship with the Company. Unless we reasonably consider that we need to use it for another related reason and that reason is compatible with the original purpose, we will not change the original purpose for collecting your personal data. It is important to be aware that we may process your data without your knowledge or consent where this is required or permitted by law. Your personal data is collected for the purposes and reasons set out below. These reasons are not mutually exclusive, and may be used by the Company under more than one heading for the same personal data:

A. It is necessary for the performance of your contract with us

We need to process your personal data in order to meet our obligations or exercise rights under your contract with the Company. Information processed for this purpose includes, but is not limited to, personal data relating to: payroll; your pension; your bank account; your postal address, email address and telephone number; administering the contract we have entered into with you; emails sent or received by you or between other employees, which are stored by the Company; any record of absence; sick pay; annual leave; family leave and pay; emergency contacts; training and development; conducting and managing performance reviews; making decisions about salary reviews and compensation; making decisions about your continued employment; making arrangements for the termination of our working relationship; reward and recognition; research and teaching; disciplinary matters; criminal convictions or barring decisions; health and safety; providing benefits to you and security. Your failure to provide us with this information may impair our ability to fulfil our obligations to you and/or our ability to comply with other legal obligations.

B. It is necessary for us to comply with our legal obligations

We need to process your data in order to meet legal obligations, such as those relating to immigration, health and safety, equal opportunities and employment legislation. Information processed for this purpose includes, but is not limited to, information relating to tax; national insurance; auto-enrolment for pension; statutory sick pay; statutory maternity, adoption, paternity and shared parental pay; family leave; work permits or immigration status; management of health and safety and equal opportunities monitoring. We are required to disclose much of this data to Government departments or agencies.

***C. It is necessary for our legitimate interests* or the legitimate interests of a third party:**

"Legitimate Interests" means the Company's interests in conducting and managing our business, including the governance and operation of the Company to ensure that we are able to manage our

employees throughout the duration of their contract with us and beyond. It may, in limited circumstances, also include the legitimate interests of a third party. Examples of such processing include (but are not limited to) the following:

- Communications;
- Internal reporting;
- Policy development;
- Business management and planning;
- Benchmarking;
- Accounting and audits;
- Administration of health and safety;
- Administration of loans and/or benefits;
- Your participation in events and other activities organised in support of Company objectives;
- To enable us to deal with and/or defend any dispute or legal proceedings including accidents at work;
- To gather evidence for possible grievance or disciplinary hearings;
- To establish whether you are suitable for the role that you have applied for;
- To enable us to monitor our business performance and protect our business interests;
- To monitor your use of our information, communication and technology systems to ensure compliance with our IT policies;
- Security;
- Maintenance of IT systems, including information security; and
- Potential conflicts of interest.

D. Where none of the other lawful reasons apply, but it is necessary to protect your life or the life of someone else.

While these situations are likely to be rare, if for example you were to become seriously unwell or have an accident during recruitment or employment, we may need to provide medical practitioners with personal data about you.

E. Consent

In certain limited circumstances we may rely on your consent to process your personal data. Where we rely on your consent, we will make this expressly clear and we will ask you to volunteer the information. We would typically rely on your consent when asking you to participate in surveys or where we ask you to share sensitive personal data with us.

9. Sharing Personal Data with Third Parties

We may share your personal data with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

We are taking steps to ensure that all third-party service providers are required to take appropriate security measures to protect your information in line with our policies. We will limit third-party service providers to use your personal data for their own purposes and will be clear with them as to the specified purposes that they are authorised to process your personal data.

10. Transfer of your personal data outside the European Economic Area (EEA)

We will not share / transfer your personal data to Countries outside the EEA.

11. Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We are putting in place procedures that deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

12. Your Rights

It is important that the personal data we hold about you is accurate and current.

Under certain circumstances, by law you have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.

Request the transfer of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact us in writing.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our HR Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

13. Review

We reserve the right to review and update this Policy at any time, and we will advise you should we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

Date last revised: 25 May 2018