****

**ReMind UK privacy notice for employees, workers and contractors**

About This Notice

ReMind UK is a registered charity focused on essential research and providing support for people with dementia, their families and carers, dedicated to improving the quality of life of everyone involved.

For us to carry out our activities and obligations as an employer we need to collect information about your actual or potential employment with us (which for the purpose of this notice includes our volunteers and Trustees). However, we recognise the importance of your privacy and ReMind UK is committed to ensuring that your privacy is protected.

For the purpose of this notice ReMind UK is the “data controller”.

This notice tells you what personal information ReMind UK collects about our employees, workers and contractors (and also includes those applying for a position with us, our volunteers and Trustees), why we need it, how we use it and what protections are in place to keep it secure.

All staff at ReMind UK receive regular, mandatory training in information governance and handling personal data.

Data protection principles

In relation to your personal data, we will:

* process it fairly, lawfully and in a clear, transparent way
* collect your data only for reasons that we find proper for the course of your relationship with ReMind UK in ways that have been explained to you
* only use it in the way that we have told you about
* ensure it is correct and up to date
* keep your data for only as long as we need it
* process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

What do we collect?

|  |  |
| --- | --- |
| **Type of information** | **Examples****please note the examples are illustrative and not an exhaustive list.** |
| **Information about you** | Name, address, date of birth, nationality, race, gender, details of any disability,work restrictions. |
| **Contact information for you** | Name, address, telephone numbers, email addresses. |
| **Emergency contact information** | Name, address, telephone numbers and their relationship to you |
| **Information to identify you** | Photographs, driving licence, passport |
| **Information about your suitability to work for us and skills and experience** | CVs, application forms, interview notes, references, qualifications, training, professional registration details, work visa ID information, pre-employment checks including criminal record checks (DBS) and credit and fraud checks |
| **Details of your employment with us** | Offer letters and acceptance of employment, employment contract. |
| **Information needed to pay you** | Bank account details, national insurance number |
| **Information to provide you with benefits and other entitlements****(pension etc)** | Length of service information, health information, leave requests |
| **Information relating to your performance at work** | Performance reviews/ appraisals, one to one meeting notes, personal development plans, targets and objectives |
| **Information relating to discipline, grievance and other employment related processes** | Interview/ meeting notes, correspondence |
| **Information relating to your work travel and expenses** | Bank account details, passport, driving licence, vehicle registration and insurance details. |

When/ how we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment/engagement, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies. Personal data is kept in personnel files or within the Company’s HR and IT system.

Why we collect and use your data

ReMind UK will process and may disclose such data for the purposes of the administration and management of your employment/ engagement with ReMind UK and/or ReMind UK business and you consent to the processing and disclosure of such data, both manually and by electronic means, both inside and, where necessary, outside the European Economic Area. Your personal data is processed by ReMind UK in relation to and with the purpose of managing your actual or potential employment or contracting agreement with us.

|  |  |
| --- | --- |
| **Reason for collecting your personal information** | **Examples****please note the examples are illustrative and not an exhaustive list.** |
| Recruitment | * To assess candidates suitability for the role
* To carry out screening, assessment and interviews
* To make offers of employment and provide employment contracts
* To carry our pre-employment checks, including checks of legal right to work in the UK, criminal record checks, and professional registration checks.
 |
| Human resources (HR, finance and other business administrative purposes) | * Organisational planning and development and workforce management
* Payroll, benefit planning and administration including salary, tax, awards, insurance and pensions.
* Workforce development, education, training and certification
* Performance management
* Problem resolution, including carrying our internal reviews, grievances, investigations and audits
* Business travel and expense management
* Business reporting and analytics
* Administration of flexible working arrangements
* Administration of employee induction and on boarding
* Work related injury and illness, including the management of Health and Safety and disabilities.
* To provide HR support
* Compliance and compliance reporting including conflicts of interest, and gifts and hospitality recording
* Risk management
* Training and quality purposes
* Arranging access to third party resources, such as (but not limited to) Bath University IT, RUH, HCRG Healthcare.
 |

|  |  |
| --- | --- |
| Security purposes | * Physical access
* Authorising, granting and administration, monitoring and terminating access to use our or third party facilities, records, property and infrastructure including communication services such as business emails/ internet and phones
 |
| Information technology administration purposes | * IT systems access control and monitoring
* IT fault reporting, management and resolution
* Systems administration, support, development, management and maintenance
 |
| Legal purposes | * To comply with our legal obligations
 |

Special categories of data

Special categories of data are data relating to your:

* Health
* sex life
* sexual orientation
* race
* ethnic origin
* political opinion
* religion
* trade union membership
* genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

* you have given explicit consent to the processing
* we must process the data in order to carry out our legal obligations
* we must process data for reasons of substantial public interest
* you have already made the data public.

We will use your special category data:

* for the purposes of equal opportunities monitoring
* in our sickness absence management procedures
* to determine reasonable adjustments

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Sharing your data

There are a number of reasons we may share your information and this can be due to:

* Our obligations to comply with current legislation
* Our duty to comply with any Court Order that may imposed

We will sometimes pass information about you to third parties, where the law allows it. For example, to Bath University to arrange your IT access, if you work in the Memory Clinic to HCRG Care Group, our commissioners, where required, to Atlantic Data so criminal record checks can be carried out (known as DBS checks).

This list is not exhaustive and staff will be notified about any new use of their data. When we enter into a contract with an external supplier we ensure that your data will be held securely.

Where we share your information we ensure that we only share the minimum necessary for the specific purpose. We do not sell your information.

How we protect your data

Appropriate technical controls are in place to store and protect personal data. We have security procedures in place to guard against unauthorised access, improper use, alteration, destruction or accidental loss of your personal information. Information is only accessible by only accessible by the HR Manager and CEO and your line manager. You should not share your (or anybody else’s) personal information unless there is a genuine business reason for doing so.

We also use a GDPR compliant self-service HR System, Breathe HR, to keep your personnel records. This is a secure system and has levels of access set out below.

* HR Manager and CEO: Can see all details
* Finance Manager: Can see Bank details
* Line Manager: Can only see the details of their direct reports including: profile details, annual leave details, sickness record, details of one to one meetings and annual appraisal.
* Staff: You can see your profile details and holiday calendar.

How long we keep your data

In line with data protection principles, we only keep your data for as long as we need it, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Retention periods can vary depending on why we need your data, and more details are available in the Data Retention Schedule on Breathe HR.

In general:

* If your application with ReMind UK is unsuccessful we will hold your information for six months from the end of the recruitment period.
* If you are employed by ReMind UK we keep your relevant data throughout your employment with us.
* If you leave ReMind UK we will keep your data for as long as necessary to satisfy the purpose for which it was collected, and within legislative guidelines. Our retention schedule which can be found on Breathe HR, has more detailed information on this.

Data will be securely destroyed when no longer needed.

How you can access your information

We aim to ensure that the information we have for you is accurate and up-to-date. You can request to see this information and if for example you believe that something is incorrect, or you do not wish us to retain it you can ask to have it have it corrected or deleted.

You can see some of the information that we hold for you on Breathe HR, but if you would like to request access to the information we hold not on this system please send your request in writing to alison.easto@reminduk.org

If you wish to raise a complaint on how we have handled your personal information you can ask us to investigate the matter. Contact alison.easto@reminduk.org

If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the Information Commissioner’s Office <https://ico.org.uk/>