

GDPR Privacy Notice

What is the purpose of this document?

At Vision Mental Health we're committed to protecting the privacy and security of your personal information.

Our Policy explains when and why we collect personal information about our employees, how we use it, the conditions under which we may disclose it to others and how we keep it secure, in accordance with the General Data Protection Regulation (GDPR).

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only 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 told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Any questions regarding this Policy and our privacy practices should be sent by email to DPO@vision-mh.com or by writing to The Data Protection Officer, Vision Mental Healthcare, Cornerstone House, Barnet Lane, Elstree, Borehamwood, Hertfordshire, WD6 3QU. Alternatively, you can telephone 02089 532573.

We respect your privacy and that of your fellow Colleagues. We therefore recognise the need for appropriate safeguards in relation to the collection, storage and processing of personal data. We aim to fully comply with the requirements of the General Data Protection Regulations.

Vision Mental Healthcare is a data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees. This notice does not form part of any contract of employment. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependents
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through biometric means such as the fingerprint clock in machines.
- Information about your use of our information and communications systems.
- Photographs.

We may also collect, store and use the following 'special categories of more sensitive personal information:

- Information about your health, including any medical condition, health and sickness records.
- Biometric data. (Fingerprints for our clock in machines)
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees through the application and recruitment process, usually directly from candidates. We may sometimes collect additional information from third parties including former employers, character references, or other background check agencies for DBS processing.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

- We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:
- Where we need to perform the contract we have entered into with you.

- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest.

Situations in which we will use your personal information

We need all the categories of information in the list above (see: *The kind of information we hold about you*) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and deducting tax and National Insurance contributions and liaising with HMRC for such issues.
- Liaising with your NOW pensions provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary meetings.
- Making decisions about your continued employment or engagement.
- Training and development requirements.
- Dealing with legal disputes involving you, or other employees, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To monitor your attendance and payroll processing (using biometric fingerprint data on our clock in machines)

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our employees).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations and in line with our data protection policy.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our data protection policy.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as your employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to absence, which may include sickness absence or family related absence, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and to manage sickness absence.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

- We will use trade union membership information to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive 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. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our [data protection policy and recruitment policy].

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions

We will collect information about criminal convictions as it is appropriate given the nature of the role you will be carrying out within Vision Mental Healthcare and where we are legally able to do so. We will collect information about criminal convictions as part of the recruitment process. We will use information about criminal convictions and offences in the following ways:

- To carry out a risk assessment as per our recruitment policy to ensure the safeguarding of the people who live with us.

Automated decision making

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in Vision Mental Healthcare.

We require third parties to respect the security of your data and to treat it in accordance with the law.

Why might you share my personal information with third parties?

We will share your personal information 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. i.e. insurance claims, NOW pensions/ HMRC/Occupational Health referrals.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within Vision Mental Healthcare. The following activities are carried out by third-party service providers: pension administration, benefits provision and administration, IT services, Occupational Health referrals, this list is not exhaustive. For any further information please contact The Data Protection Officer DPO@vision-mh.com

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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

We have put in place procedures to 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.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from The HR Department. 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 information 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 of the company we will retain and securely

destroy your personal information in accordance with our data retention policy or applicable laws and regulations.

Rights of access, correction, erasure and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your time working with us.

Your rights in connection with personal information

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

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information 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 information. This enables you to ask us to delete or remove personal information 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 information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information 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.
- Request the restriction of processing of your personal information, This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact The Data Protection Officer in writing. (email DPO@vision-mh.com)

No fee usually required

You will not have to pay a fee to access your personal information (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

What we may need from you

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 information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information 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 The Data Protection Officer [email: DPO@vision-mh.com](mailto:DPO@vision-mh.com) 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.

Data protection officer

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. We do ask that if you have any issues or complaints relating to the handling of your data that you contact the DPO in the first instance to that we can deal with your complaint.

Responsibilities of employees

It is important that each of us takes responsibility for data protection. Please be mindful when handling confidential information and any personal data to ensure all Company policy and procedures are adhered to. If in the event an employee is in breach of our Data Protection Policy this may constitute misconduct and will be dealt with under the Company's disciplinary and grievance procedure.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact The Data Protection Officer [Email: DPO@vision-mh.com](mailto:DPO@vision-mh.com)

I, _____ (employee), acknowledge that on _____ (Date), I received a copy of Vision Mental Healthcare's Privacy Notice for employees and that I have read and understood it.

Print Name:

Signature: