Level 23, 215 Adelaide Street
Brisbane QLD 4000
P 07 3340 9000
ABN 45 683 963 644

Privacy Policy

The Vertaview Group which includes Vertaview Limited ("**we**", "**our**" and "**us**") and its subsidiaries are leaders in high needs disability support and mental health services, creating opportunities and championing possibilities for people with disability and mental illness. The Vertaview Group is committed to values of transparency, trust, and security with respect to our use and storage of your personal information.

We have obligations as to how we collect, hold, use and disclose personal information under the *Privacy Act 1988* (Cth) (the **Privacy Act**) and the Australian Privacy Principles (**APPs**).

The purpose of this Privacy Policy (**Policy**) is to inform you about the manner in which we collect, use and manage personal information in Australia, including when you interact with our websites and services.

This Policy appears on our websites, and copies of this Policy will be made available free of charge to any person who requests it.

By supplying us with your personal information, you are agreeing to be bound by this Policy and consent to us collecting, using, storing and disclosing that information (within and outside Australia) in accordance with this Policy.

You agree and acknowledge that you provide us with your personal information voluntarily. Once you provide your personal information to us, you are no longer anonymous to us. Where possible, we will indicate which fields are required and which fields are optional for you to fill in.

What is personal information?

Personal information is defined in the Privacy Act to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

Personal information can include sensitive information. *Sensitive information* is defined in the Privacy Act as information or an opinion about a person's race, ethnic origin, political opinions, membership of political associations and trade associations, religious or philosophical beliefs, sexual orientation or practices, criminal record, health information, genetic information about an individual that is not otherwise health information, biometric information that is used for the purpose of automated biometric verification or biometric identification and biometric templates.

Personal information can also include credit information.

What kinds of personal information do we collect and hold?

The kinds of personal information we collect and hold about you depends on our relationship with you and may include:

1. your full name, date of birth, age, and gender;
2. contact information, including phone numbers, addresses, email addresses;
3. information contained in the documents we collect to verify your identity;
4. personal and emergency contact information;
5. your communication preferences;
6. technical and behavioural information about your activity associated with our websites and services;
7. information about the IP address and device that you use to access our website;
8. marketing information, including preferences for communications and consent records;
9. information provided when you correspond with us; and
10. updates to information you have already provided to us.

If you are a customer, for us to provide services to you, we may also collect:

1. information about how you use our services;
2. any information contained on recordings of our interactions;
3. information on personal issues and experiences and relationships;
4. family background;
5. health and medical information;
6. information about your goals, funding, and how we can support you;
7. information about your racial or ethnic origin;
8. information about your sexual orientation or practices; and
9. information about your health and any disabilities you may have.

If you are a current employee or have applied for a position with us, we will also generally collect:

1. your job title or position;
2. the information contained within your application and CV/resume;
3. information collected during an interview, or from a reference;
4. personal information derived through testing (including psychometric or aptitude testing);
5. copies of licences and other certificates and qualifications;
6. information included in a passport, birth certificate, visa or other documentation demonstrating a right to work in Australia; and
7. tax file number and country of residency information.

How do we collect and hold your personal information?

We collect your personal information:

1. from you when you provide your personal information to us, including through face to face meetings, over the telephone, by completing forms, agreements, surveys, and applications, including online, in person, in writing, in surveys, through social media or over the telephone;
2. from a member of your family, next of kin, guardian, or authorised representative where it is unpractical or unreasonable to collect the information from you;
3. pursuant to an order of an Australian court or tribunal that authorises us to be provided with the information;
4. when you apply to become an employee, consultant, contractor or supplier to us;
5. when you place an order for our goods or services over the phone or in-store;
6. when you attend forums, events or conferences;
7. from third parties, such as doctors, nurses, allied health professionals, and other service providers whom you have provided consent to share information with us;
8. from our suppliers, contractors, and related entities;
9. from registration and event attendance;
10. from government departments, such as the National Disability Insurance Agency;
11. from public records and other publicly available sources;
12. when we provide you with support; and
13. if you are a current employee or have applied for a position with us:
    - from referees when they provide references;
    - academic institutions or training and certification providers;
    - providers of licence and background-checking services;
    - recruiters and other service providers who assist in the engagement process; and
    - other publicly available sources such as social media platforms.

If you provide us with sensitive information about other individuals, such as health information, please ensure that the individual or the individual's representative is aware of the disclosure and that he or she consents to the disclosure to us as well as to the handling of their personal information in accordance with this Policy. Otherwise you must not provide us with any sensitive information about other individuals.

If you access our websites, we may collect additional personal information about you in the form of an IP address and domain name. If you do not want information to be collected through the use of cookies or traffic measurement software, your device and/or browser may enable you to delete or "turn off" cookies or the measurement software features. However, some or all parts of our website may not function correctly if such features are disabled.

In addition, our websites may contain links to other websites. We are not responsible for the privacy practices of linked websites and linked websites are not subject to our privacy policies and procedures.

We will usually notify you about instances of collection of your personal information from third parties in advance, or where that is not possible, as soon as reasonably practicable after the information has been collected.

Upon request, we will provide you with the source of your personal information, unless it is impracticable or unreasonable to do so.

Why do we collect and how do we use your personal information?

We collect your personal information (including sensitive information) so that we may:

1. provide you with the highest quality services, including disability and mental health support services, and support coordination services;
2. operate and facilitate your use of our websites;
3. manage our relationship with you;
4. communicate with you;
5. provide you with information about services that we, or our related entities and other organisations that we have affiliations with, offer;
6. investigate or report suspected unlawful activity;
7. protect someone's life, health, safety or welfare; and
8. comply with our legal and regulatory obligations.

For prospective employees, consultants, contractors and suppliers, we collect your personal information to assess your suitability to work with us.

We also collect your personal information to conduct our business, to provide and market our goods and services or the goods or services of third parties, to improve our goods and services or to enable you to attend our events and conferences.

We may use your personal information in artificial intelligence models under controlled secure conditions that are designed to protect your personal information to:

1. summarise your interactions with us; or
2. improve the services we provide.

What happens if you don’t give us your personal information?

If you would like to access any information or any of our goods and services on an anonymous basis or using a pseudonym, please tell us. If this is possible and lawful, we will take all reasonable steps to comply with your request. However, if you do not provide us with your personal information, we may not be able to provide you with our goods or services or to engage or employ you.

Who we disclose your personal information to?

We use systems and processes to store your personal information securely and we train our staff to secure your data. We may disclose your personal information to others where we are required or authorised by law or where you have provided consent for us to do so.

We may also disclose your personal information:

1. to our related entities;
2. to consultants and suppliers working with us in providing professional, business, technology and corporate services;
3. to relevant government agencies which regulate or oversee our services, operations and activities;
4. to a member of your family, next of kin, guardian, authorised representative, the police, ambulance services, hospitals, or emergency medical centres;
5. to our employees or other service providers involved in providing support to you, such as nurses and allied health practitioners, or administrative staff;
6. law enforcement officers, regulators, courts and government agencies, if permitted or required:
    - by law, regulation, court order or other legal process;
    - to assist in the prevention or detection of crime; or
    - to prevent a threat to any person's life, health or safety;
7. to our insurers;
8. our professional advisers (e.g. lawyers and accountants); and
9. any purchaser or prospective purchaser of our business, including in the case of bankruptcy, a merger, acquisition, reorganisation, sale of assets or assignments, or due diligence in respect of any such transactions.

For prospective employees, consultants, contractors, and suppliers, we may disclose your personal information to third parties to assist us in considering your suitability to work with us and for managing our employment or engagement of you.

We may also use your personal information to provide you with information about our products, goods, and services.

Disclosure of personal information overseas

Our servers are hosted in Australia.

We are not likely to disclose your personal information overseas. However, we are assisted by a variety of external service providers and we may in the course of our business disclose your personal information to them to operate our business, these service providers may be located in the United Kingdom; the Republic of Ireland; the United States of America; Canada; Sweden; Germany; Saudi Arabia, New Zealand, India, Singapore, the Philippines, and the Netherlands.

If we disclose personal information to an overseas recipient, we will ensure that there are appropriate measures in place to protect your personal information.

You consent to any disclosure of your personal information outside of Australia on the understanding that if the overseas recipient handles the personal information in breach of the APPs, the entity will not be accountable under the Privacy Act, and you will not be able to seek redress under the Privacy Act. The overseas recipient may not be subject to privacy obligations or any principles similar to the APPs. Individuals may not be able to seek redress in some overseas jurisdictions, and overseas recipients may be subject to a foreign law that could compel the disclosure of personal information to a third party, such as an overseas authority.

Marketing and advertising

We will never use or disclose any sensitive information for direct marketing purposes without your consent.

We may use and disclose your personal information (other than sensitive information) to provide you with information about products or services offered by us or other parties.

To the extent we use your personal information for direct marketing purposes, we will provide you with the ability to opt-out of such uses, if you do not wish to receive such communications. To opt-out of being on such call, SMS, e-mail, or other communication lists, please follow the directions on such communication to unsubscribe, and we will ensure you do not receive such communications in the future.

Data integrity

We may combine the information you give to us and information we automatically collect about you to maintain and improve the accuracy of the records we hold about you. We may also use the combined information about you to form a view on what services we think you, or others similar to you, may want or need to target our marketing closer to your interests.

We endeavour to ensure that all personal information that we hold is accurate, complete, and up-to-date. To assist us with this, individuals should contact us if any of their personal information changes, or if they believe that the personal information that we have is not accurate or complete.

When personal information that we collect is no longer required by us, we will destroy or de-identify that personal information unless we are required by a law or a court/tribunal to retain the personal information.

We may retain personal information for so long as it is required for any of our reasonable business purposes, for the prevention of fraud, for insurance and governance purposes, or for the purposes of complying with any relevant regulations or laws.

Security

We take reasonable steps (including technical and organisational measures) to ensure that your personal information is stored safely and to protect it from misuse, interference, loss, unauthorised access, modification or disclosure, including the following:

1. electronic and physical security measures;
2. maintaining strict access controls and endpoint security;
3. ensuring that staff access is role-based and monitored, and we maintain an information security management system;
4. ensuring that all staff undergo privacy training; and
5. ensuring that we review threats and incidents, and implement policy updates.

We hold your personal information electronically on cloud-based storage and may retain physical copies of any original documents that you provide us.

Credit and debit card information that you provide to us by telephone or online is not kept on file. You will need to provide us with your credit card information each and every time you purchase from us.

While we take reasonable steps to protect the personal information that we hold from misuse, loss, unauthorised access, modification or disclosure, you should be aware that no system is completely secure against cyber attack.

In addition, the open nature of the internet is such that information exchanged via the internet may be accessed and used by people other than those for whom the data is intended. Any information sent via the internet is sent at the sender's risk.

You should contact us immediately if you believe that there has been unauthorised access or disclosure with respect to any personal information that we hold about you.

Government-related identifiers

We do not use any government related identifiers, such as Medicare, driver's licence or passport numbers, as our own internal identifier of any individual. We will not use or disclose any government related identifiers other than in accordance with the Privacy Act.

De-identified data

You consent to us using and disclosing your de-identified data (information that no longer identifies you) for any purpose, including, without limitation, statistical analysis, product or service development, marketing and business planning, training of AI or any other commercial purpose. We undertake technical measures to ensure that this data cannot be associated back to you.

Automated decision-making systems

All decisions we make that affect your rights will be made by a person. However, to ensure that we provide the most appropriate services within reasonable timeframes we may process your name, address, or health information using a computer program to do something that is substantially and directly related to making a decision that could significantly affect your rights or interests. We have set out some examples below:

1. we may use tools which analyse the information you give us about your needs and give us an idea about what support categories meet your needs prior to our staff deciding which support categories are appropriate to offer you;
2. after obtaining your express consent, we may use computer scribe tools to generate a transcript or summary of conversations with us, we may reference this transcript when making decisions about the services we propose to offer to you; and
3. we may use a tool that recommends which workers are most appropriate to care for a particular customer, based on criteria such as skills, availability, client preferences, continuity of care, and travel distance, however our staff will make the final decision about which of our workers are appropriate to provide care.

Access to and correction of information

You are entitled to have access to and seek correction of any personal information that we may hold about you, subject to the grounds for refusal under the Privacy Act. We prefer that requests for access to, or to update or correct, your information be in writing outlining the details of your request. Such requests should be addressed to our Privacy Officer via the details provided in this Policy.

Requests for access to information

We do not impose a charge for making a request for access. However, we may charge for reasonable administrative costs incurred in providing access.

We will take appropriate steps to verify your identity (or verify that you act as an authorised agent of the individual concerned) before granting access to your personal information.

We will respond to your request for access to your personal information within a reasonable time after you make the request and, if access is granted, access will be provided within 30 days from your request. If we deny your request, we will provide you with a written notice detailing the reasons for the refusal and the process for making a complaint about the refusal to grant your request.

Where your request for access is accepted, we will provide you with access to your personal information in a manner, as requested by you, providing it is reasonable to do so.

Requests for correction of information

We do not impose any charges with respect to requests to update or correct your personal information.

Your request for correction will be dealt with within 30 days, or such longer period as agreed by you. If we deny your request, we will provide you with a written notice detailing reasons for the refusal and the process for making a complaint about the refusal to grant your request.

We will accept your request for correction of your personal information where we are satisfied that it is inaccurate, out-of-date, incomplete, irrelevant, or misleading. Upon accepting a request for correction of your personal information, we will take all steps that are reasonable in the circumstances, having regard to the purpose for which your information is held, to correct your personal information.

If we refuse to correct your personal information, you have the right to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. We will take such steps as are reasonable in the circumstances to associate that statement with all records we hold that contain the relevant information.

Where to access further information and how to make complaints

The Vertaview Group treats your privacy seriously. Our Privacy Officer handles any privacy related queries, requests, or complaints, including complaints about a breach of this Policy, the Privacy Act or the APPs. You may also contact our Privacy Officer to access the personal information we hold about you or request the correction of that information.

Our Privacy Officer can be contacted at:

Ph: 07 3340 9000 or 1300 135 886

Email: privacy@vertaview.org.au

Post: PO Box 4013, Eight Mile Plains Qld 4113

We will not impose any charge for making a complaint, or for dealing with the complaint. Once a complaint has been lodged, our Privacy Officer will consider your complaint and respond as soon as reasonably possible, but not more than 30 days from receiving the complaint.

If, after this process, you are not satisfied with our response, you can submit a complaint to the Office of the Australian Information Commissioner (**OAIC**).

Office of the Australian Information Commissioner

The contact details for the OAIC are:

Postal address: GPO Box 5218
Sydney NSW 2001

Telephone: 1300 363 992

Email: enquiries@oaic.gov.au

For more information on privacy, see the OAIC's website at: http://www.oaic.gov.au.

Effect of this Policy

This Policy may be varied by us from time to time.

This policy does not create any rights or obligations that you can legally enforce against us beyond the rights and obligations provided under the Privacy Act.