

Privacy and Confidentiality Policy



Policy: Privacy and Confidentiality Policy

Policy number: PC v7

Date adopted: Oct 2018

Authorised by: Lee-Anne Morse

Date last reviewed: Jul 2024

Reviewed and updated by:
David Semgreen

Date of next review: Oct 2026

Major changes since last review:

Policy context: This policy relates to:

Human Services Quality Framework

Standard 1: Governance and Management
Indicator 7: The organization has effective information management systems that maintain appropriate controls of privacy and confidentiality for stakeholders

Other Standards

Queensland Information Privacy Act 2009
Australian Privacy Guidelines
NDIS Practice Standards 2018
NDIS Act 2013
NDIS Code of Conduct 2019

Legislation or other requirements

Disability Services Act Qld 2006
Commonwealth Disability Discrimination Act 1992
Commonwealth Disability Services Act 1986
Guardianship and Administration Act 2000
Mental Health Regulation 2002
Power of Attorney Act 1998
Home and Community Care Act 1985
Racial Discrimination Act 1975
Sex Discrimination Act 1984
Queensland Information Privacy Act 2009
Commonwealth Privacy Act 1988



1. Purpose: Why do we have a privacy policy?

Beyond the Spectrum is committed to providing an effective and high-quality service that maintains appropriate accountability and transparency. As part of our services, we must collect, safely store and sometimes share relevant personal information about our primary persons and their stakeholders. It is important that we are consistent and careful in the way we manage this collected information in regard to - what is written and/or said about a primary person and stakeholders and how we decide who can see or hear this information.

Our primary persons, their stakeholders and staff/affiliates have legislated rights to confidentiality and privacy, and to accessing their own records. It is essential that we protect and uphold these rights, and that we act correctly in those circumstances, where the right to confidentiality or privacy may be overridden by other considerations.

2. Scope

This policy will apply to all written, verbal and electronic personal or sensitive information relating to primary persons, stakeholders, all staff/affiliates, including contractors and volunteers, unless, or in special circumstances where the law allows or dictates an exception.

To uphold the rights of primary persons, stakeholders, staff/affiliates and volunteers to confidentiality and privacy, each staff and management member needs an appropriate level of understanding about how we meet our legal obligations:

- restricting access to confidential information regarding primary persons, stakeholders, and staff consent to not share information about them
- our processes for providing information to people accessing, or working in, our services
- avoiding/minimising risk of this information being accessed by non-authorised persons, either by intentional or accidental means

2.1 Definitions

Personal information (as defined by the Privacy Act 1988)

Is 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.

Sensitive information (As defined by the Privacy Act 1988)

Is information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health, genetic or biometric templates, that is also personal information.

Confidentiality

Implies the relationship of confidence between the organisation and individuals.



3. Policy statement: Our commitment

Beyond the Spectrum recognises the essential right of individuals to have their information collected, protected and administered in ways which they would reasonably expect. This means that we ensure no personal information about a primary person, stakeholders, staff person/affiliate or volunteer is shared with anyone, on purpose or by omission, unless we have informed consent from the primary person or guardian or in special circumstances, where the law allows or dictates an exception. On the other hand, *Beyond the Spectrum* will make accessible to the primary persons any information that relates to them and processes by which to provide informed consent on information release and to correct information held. *Beyond the Spectrum* is committed to delivering services, whereby Privacy and Confidentiality values are reflected in, displayed and supported by our core values and philosophies within all policies, which are compliant with the Privacy Act 1988 (C) and meets relevant principles of the *Queensland Information Privacy Act 2009*.

Beyond the Spectrum has adopted the following principles contained as minimum standards in relation to handling personal information according to the principles of privacy and confidentiality. *Beyond the Spectrum* will:

- Meet legal and ethical obligations as employees, volunteers and managers in relation to protecting the privacy and confidentiality of primary persons and their stakeholders
- Provide primary persons and their stakeholders with information about their rights regarding privacy and confidentiality
- Take account of and show respect for any relevant cultural or religious requirements of primary persons and their stakeholders and make reasonable consideration and adjustments, where indicated or requested
- Ensure privacy and confidentiality for primary persons and their stakeholders when collecting, storing, using or disclosing personal information or discussing matters of a personal or sensitive nature with staff or volunteers
- Collect only information which the organisation requires for its primary function
- Ensure that the primary person and their stakeholders are informed as to why we collect information and how we administer the information gathered
- Use and disclose personal information only for our primary functions or a directly related purpose, or for another purpose with the person's informed consent
- Store personal information securely, protecting it from unauthorised access
- Provide stakeholders with access to their own information, and the right to seek its correction

To uphold the above, each staff member and volunteer needs an appropriate level of understanding of:

- confidentiality, limits to confidentiality and obtaining clients, staff and volunteer consent to share information about them
- our processes for providing information to people using, or working in, our services



3.1 Company Device Limitations

Using personal accounts

We limit and monitor our employee's usage of the internet on Beyond The Spectrum owned IT equipment. This includes but not limited to:

- Facebook
- Twitter
- YouTube
- Tik Tok
- Instagram
- Email

If you're using your accounts for personal purposes, you may easily get side-tracked and forget your supposed to be working. Personal accounts are not to be accessed via company IT equipment unless approved by the appropriate supervisor and IT Manager.

We ask you to be careful when posting on social media, too. We can't restrict what you post there, but we expect you to adhere to our confidentiality policies at all times. We also caution you to avoid violating our anti-harassment policies or posting something that might make your collaboration with your colleagues more difficult (e.g. negative opinions against groups where colleagues belong to).

We advise our employees to:

- **Ensure others know that your personal account or statements don't represent our company.** You shouldn't state or imply that your personal opinions and content are authorized or endorsed by our company. We advise using a disclaimer such as "opinions are my own" to avoid misunderstandings
- **Avoid sharing intellectual property** like trademarks on a personal account without approval or client information. Confidentiality policies and laws always apply
- **Avoid any defamatory, offensive or derogatory content.** It may be considered as a violation of our company's anti-harassment policy, if directed towards colleagues, clients or partners

Our right to monitor and Investigate

If you use any personal accounts on any computer or device that is owned by Beyond The Spectrum PTY LTD the accessed account, information or data will become the property of Beyond The Spectrum PTY LTD. This does not mean that we will own your personal account, however any information or data accessed on the computer or device will become the property of Beyond The Spectrum PTY LTD.



Computers and devices

Any of the following computers and devices owned by Beyond The Spectrum PTY LTD may include but not limited to:

- Desktop Computers and Apple Computers
- Laptops, MacBooks, Tablets and iPads
- Mobile and desktop phones
- Servers and network infrastructure

Representing our company

Some employees represent our company by handling corporate social media accounts or speak on our company's behalf. When you're sitting behind a corporate social media account, we expect you to act carefully and responsibly to protect our company's image and reputation. You should:

- **Be respectful, polite and patient**, when engaging in conversations on our company's behalf. You should be extra careful when making declarations or promises towards customers and stakeholders
- **Avoid speaking on matters outside your field of expertise** when possible. Everyone should be careful not to answer questions or make statements that fall under somebody else's responsibility
- **Follow our confidentiality policy** and observe laws on copyright, trademarks, plagiarism and fair use
- **Inform our *Marketing department*** when you're about to share any major-impact content
- **Avoid deleting or ignoring comments** for no reason. You should listen and reply to criticism
- **Never post discriminatory, offensive** content and commentary
- **Correct or remove** any misleading or false content as quickly as possible

Disciplinary Consequences

We will monitor all social media postings on our corporate account.

We may have to take disciplinary action leading up to and including termination if employees do not follow this policy's guidelines. Examples of non-conformity with the employee social media policy include but are not limited to:

- Disregarding job responsibilities and deadlines to use social media at work
- Disclosing confidential information through personal or corporate accounts
- Directing offensive comments towards other members of the online community



4. Procedures

Beyond the Spectrum recognises its responsibilities to uphold the principles of privacy and confidentiality for primary persons and their stakeholders in a manner which complements our client charter, our code of conduct and complies with; and always reflects current legislation.

The Privacy Act 1988 provides protection of personal information and outlines privacy principles which set the basic rules for handling peoples information. The principles provide the information-handling standards for things such as collecting, using and disclosing personal information as well as keeping information secure, paying attention to data quality and accuracy, being open about the collection and information handling practices, providing access to personal information, providing anonymity where possible and providing protection when transferring personal information overseas.

We manage our obligations in relation to protecting the privacy of our primary persons and their stakeholders by being transparent with people about how we handle their information and to develop trust relationships with primary persons and their support network.

4.1 Primary Persons

Beyond the Spectrum collects personal or sensitive information for the purpose of delivering quality direct services, administering processes associated with service delivery e.g. referrals, meeting any requirements for government funding, monitoring or evaluating the services we provide, to comply with legal obligations or to produce annual reports or for research purposes. The nature and extent of the information collected by *Beyond the Spectrum* varies depending on the individual's interaction with us. This information may be collected by *Beyond the Spectrum* using in-person interviews, service entry processes, online or electronic communications, questionnaires or over the telephone. These processes are subject to regular internal review and form part of Beyond the Spectrum's continuous improvement program to deliver quality, appropriate and inclusive services to our primary persons and their stakeholders.

Such information may include:

- Contact details (name, address, email, etc.)
- Personal details (date of birth, gender, income, emergency contacts, etc.)
- Information on personal issues and experiences, areas of interest or relationships
- Family background or supports that participants may have in the community
- Cultural or religious requirements and adjustments that account for these sensitivities
- Health information and/or medical history
- Criminal history
- Credit card or bank account details
- Server address and online visit information



In protecting the privacy and confidentiality of primary persons and their stakeholders, we ensure they are well informed about their rights and that we take our responsibilities seriously.

Beyond the Spectrum staff will:

- Be trained in the Privacy and Confidentiality policy and how this policy relates to service provision at *Beyond the Spectrum*. Training will be recorded in the training register and held on the employee's file
- Gain consent for *Beyond the Spectrum* service delivery of support coordination during the service entry procedure for a primary person and their stakeholders
- Inform the primary person, or guardian, what information they are collecting, why the information is needed as part of their service delivery, and how long this information will be kept.
- Provide the primary person and their stakeholders with a Privacy Statement that outlines how *Beyond the Spectrum* exercises its responsibilities under the Australian Privacy Principles (see section 4.5)
- Only record information in a primary person's file if it is necessary for the person's service provision, now or in the future
- Any other information, photographs or films will only be retained or used if the primary person or guardian provides informed consent. Photographs or films will be used with consideration for the best interests of the primary person and their stakeholders and will not, whole or in part be provided, shared or sold to any third party
- *Beyond the Spectrum* may keep case notes, including observations about people's progress, activity participation and enjoyment, any changes in behaviour, any incidents, feedback or requests, as well as file correspondence or reports
- All information recorded will be accurate and factual, opinion or hearsay will be avoided or clearly indicated. Information will be clear, brief, legible and easy to understand and will be traceable through signature and date on a person's file. Primary persons, or their guardians, will know where their file is kept and can see and review their personal information upon request. *Beyond the Spectrum* will support primary persons or guardians in accessing their stored information and will explain the information written if requested
- Primary persons, or their guardians, can have request to correct information in their files through written request to the CEO and this request cannot be unreasonably denied
- Only the CEO has the authority to reasonably deny a request to access or correct file information. In this instance, written notification of the denial to access or correct information must be given to the individual who requested such information with reasons why access or corrections have been denied and rights of the individual to appeal their decision and how this might be carried out.
- Appeal reviews will be carried out by a mutually-agreeable independent reviewer who is suitably qualified to review the request, the decision and the circumstances around the decision and provide both the individual and *Beyond the Spectrum* with an outcome
- *Beyond the Spectrum* will not allow any third party to access a person's file unless the primary person or guardian provides informed consent. Third party access must also have the approval of the CEO



- *Beyond the Spectrum* will retain primary person files as required by current Queensland legislation. If a person is transferring to another service, a copy of the file may be provided with informed consent from the primary person or their guardian
- Sharing of private information about a primary person or their stakeholders to a third party will require the approval of the CEO. The CEO will ensure a record of the shared information including what information was shared, why the information was requested and record of informed consent from the primary person or their guardian is stored in the client file

When talking to primary persons or their guardians about information of a private or personal nature, *Beyond the Spectrum's* staff will:

- Ensure they are the most appropriate staff member to be interviewing or discussing information of a private or personal nature
- Provide options for physically separated spaces, such as private offices or interview rooms or at the client's home, if requested
- Provide options for private telephone calls to ensure personal information cannot be overheard
- Explain to the individual that they may request a support person or advocate in attendance, especially if there are cultural or religious requirements that have been identified on file. Requests for a support person or cultural and religious adjustments will not be unreasonably denied
- Primary persons or their guardians will have access to any notes from the meeting, during or after the meeting or after the notes are placed on their file in line with the Australian Privacy Principles. A primary person or guardian may request access to their file through written request to the CEO and this request will not be unreasonably denied

4.2 Staff and Beyond the Spectrum affiliates/stakeholders

Beyond the Spectrum collects personal information from applicants, employees, volunteers and contractors (collectively known as staff), for the purpose of recruitment or administering their employment conditions. *Beyond the Spectrum* recognises its responsibilities to uphold the principles of privacy and confidentiality for staff in a manner which complies with relevant legislation. We manage our obligations in relation to protecting the privacy of staff by being transparent with people about how we handle their information.

The employee is to be informed of what information is collected, why it is being collected. This information may be collected by *Beyond the Spectrum* using in-person interviews, service entry processes, online or electronic communications, questionnaires or over the telephone. These processes are subject to regular internal review and form part of *Beyond the Spectrum's* continuous improvement program.



The nature and extent of the information collected by *Beyond the Spectrum* varies but may include:

- Contact details (name, address, email, etc.)
- Personal details (date of birth, gender, income, emergency contacts, etc.)
- Information on personal skills, work experiences or academic qualifications such as provided by the employee in their resume or covering letter or gained throughout their employ
- Interview or reference check records as part of the recruitment process
- Records on performance development or management of performance
- Health screening information, Police Checks, Positive Notice Cards
- Bank account details and superannuation details
- Taxation details including but not limited to TFN and ABN
- Online usage information

All personal information recorded will be accurate, factual, complete and up-to-date. Records and notes will be clear, brief, legible and easy to understand and will be identifiable back to the person entering information onto the file.

Beyond the Spectrum will retain employee files as required by current Queensland legislation, however we will not allow any third party to access an employee's file or information contained within these files unless the employee provides informed consent. For example: If a person is transferring to another service, a copy of the file may be provided with informed consent from the employee. A legal requirement to disclose personal information may override the Privacy Principles on which this policy is based, these exemptions to disclosure are outlined in section 4.4

Employees have the right to know where their personal information is kept and request to view their own information on held by *Beyond the Spectrum* related to their employment. Employees have the right to review and correct information in their files through written request to the CEO.

Separate work mobile phone numbers are recommended for individual employees. Work mobile numbers may be given out in the course of service delivery but personal phone numbers are considered private information and are not to be disclosed without the express consent of the employee. Work phones are expected to be on, charged and available to call and text during rostered work hours, including on call hours, and at other times at the discretion of the employee.



When talking to employees about information of a private or personal nature related to their employment, performance or contracts, management will:

- Ensure they are the most appropriate staff member to be interviewing or discussing information of a private or personal nature
- Provide options for physically separated spaces such as a private office or room
- Provide options for private telephone calls to ensure personal information cannot be overheard
- Explain to the employee that they may have a support person or advocate in attendance, or adjustments may be made for cultural or religious reasons, requests for a support person or cultural and religious adjustments will not be unreasonably denied
- Employees will have access to any notes from the meeting, during or after the meeting or after the notes are placed on their file in line with Australian Privacy Principles through written request to the CEO

4.3 Overall measures

Beyond the Spectrum ensures that safeguards are in place to protect the personal information it administers against loss, interference, unauthorised access or disclosure, modification or other misuse. These safeguards include reasonable physical and technical steps for both electronic and hard copy records. Some of these include, but are not limited to:

- *Beyond the Spectrum* will keep hardcopy primary person and employee files secure in a locked cabinet, away from public areas, and will make sure only staff who require file access in the course of their expected duties are able to see and/or access them
- Positioning electronic equipment so that they cannot be seen or accessed by unauthorised persons, including being aware of telephone conversations that may be overheard by other staff or participant stakeholders
- Electronic files will be secured using password protection on all computers and mobile devices, electronic encryption of files stored within Next Cloud as well as anti-viral software, malware protection and firewalls to restrict unauthorised use through internet security software such as Trend Micro Internet Security
- Traceability of records including attributing author and date to handwritten documents
- Disposing of records securely, when they are no longer required and transferring them to a more appropriate agency in accordance with the confidential information policy.



4.4 Exemptions for disclosure

A legal requirement to disclose personal information may override the Privacy Principles on which this policy is based; this is known as a 'duty of care'.

Situations where this may occur include the following:

- Where there is serious risk of abuse or physical harm to the primary person or other person, including stakeholders, the general public and employees
- Where the disclosure is required under Australian law
- Where the individual would reasonably expect us to use or give that information, e.g. referral processes
- When the disclosure is necessary by or for a law enforcement agency (e.g. prevention, investigation, prosecution or punishment of criminal offences, preparation or implementation of a court or tribunal order.)

If a legal need for disclosure arises, the employee will refer the matter to the CEO, who will assess the request and approve the disclosure of information. This approval will also be communicated to the individual, unless such advice to the individual is not allowed by legislation and placed on the individual's file.

4.5 Privacy Statement

Personal information collected by *Beyond the Spectrum*

Beyond the Spectrum's service provision is protected by the *Information Privacy Act 2009*. Personal information is any information that can be used to identify you and includes sensitive health information.

Beyond the Spectrum follows the Australian Privacy Principles contained in the Privacy Act in handling personal information from primary persons/beneficiaries, business partners, donors, members of the public and other *Beyond the Spectrum's* stakeholders (including members, contractors, volunteers, employees, candidates for volunteer work and prospective employees).

Beyond the Spectrum has developed a Privacy Policy to protect your privacy. The Policy is available in hard copy on request, or may be downloaded from our website, and contains detailed information about *Beyond the Spectrum* responsibilities, your rights, and the information that may be collected by us and how it would be used.



The primary purpose for collecting personal information from you is to provide disability services, including planning, funding, monitoring and evaluating our services. The kind of personal information we collect will depend on your relationship with *Beyond the Spectrum* (e.g. as a primary person, business partner, employee, contractor, volunteer or member, on line user).

We usually collect personal information directly from you. However, we sometimes collect personal information from a third party such as an authorised representative or from a publicly available source, but only if:

- You have consented to such collection or would reasonably expect us to collect your personal information in this way, or if it is necessary for a specific purpose

We only collect personal information for purposes that are reasonably necessary for one or more of our functions or activities.

Your personal information may be used to:

- Provide you with goods or a service;
- Provide you with educational information on disability care and awareness;
- Report to government or other funding bodies how the funding is used;
- Process donations, payments or purchase and provide receipts;
- Communicate with you about how your donation is used or about *Beyond the Spectrum* Therapy and Respite Services, causes, events, products and services, which we believe may be of interest to you;
- Respond to your feedback or complaints; and/or answer your queries

It may also be used for:

- Any other purpose, or directly related purposes as requested for which you provided informed consent

Please be assured that wherever possible *Beyond the Spectrum* uses information in a de-identified form. Personal information will not be disclosed to third parties without your permission, except where permitted or required under the Privacy Act.

We take steps to protect all personal, sensitive and health information and government related identifiers held by *Beyond the Spectrum* against misuse, interference, loss, unauthorised access, modification and disclosure.

You can access the personal information that we hold about you, and you can ask us to correct the personal information we hold about you. For more information, see our Privacy Policy or contact us at:

Email:
admin@beyondthespectrum.com.au

Mail:
PO Box 1279, Hervey Bay
QLD, 4655



5. Other related policies and procedures

Documents related to this policy	
Related policies	<ul style="list-style-type: none">• Staff Recruitment and Training Policy• Code of Conduct• Service Delivery Policy• Client Records Policy
Forms or other organisational documents	<ul style="list-style-type: none">• Service Agreement• Mission Statement• Blue Card – Training – License Register

6. Review processes

Policy review frequency: At least annually	Responsibility for review: CEO
<p>Review process:</p> <p>Review will be carried out by the CEO in consultation with staff. It is expected that the review process will take one month and changes will be recorded using a numerical system. Approval will be undertaken by the CEO and outlines of major changes will be noted at the beginning of the new version before dissemination to staff.</p>	
<p>Documentation and communication:</p> <p>Review of the policy will be communicated through email notification to each staff member after being stored electronically and printed at the main office.</p>	
<p>Key Questions for Review:</p> <p>Is the policy being implemented? Are procedures being followed? Is the policy clear? What has changed or trends have emerged that may prompt a change to the policy? Have stakeholders had difficulty with any aspect of the policy? Can their concerns be resolved? How does the policy compare with that of similar organisations?</p>	

