Privacy and Information Management Policy

Policy statement

Parent to Parent Association QLD Inc (P2P) is committed to respecting the Participant's right to privacy and confidentiality and ensuring that all information collected is protected.

This policy outlines what information is collected, how personal information is managed and how P2P collects, stores, uses, and disposes of personal information in accordance with relevant legislation.

This policy supports P2P to apply National Standards Disability Services Standards: 1. Rights and Responsibilities (Privacy and Dignity); 3. Provision of Supports (Access to Supports)

Participants will be notified of the availability of, and their right to access, this policy when they first use P2P services. Personnel will ensure they have understood it and know that the Privacy Policy is also located on the P2P website.

Scope

All personnel, whether paid employees, contractors, volunteers or business partners, are responsible for working within the policy and reporting when privacy breaches occur or are at risk. It is the responsibility of the Board via the CEO to ensure this policy is in place and adhered to.

Principles

P2P strongly believes that everyone has a right to privacy and confidentiality. Everyone has a right to control who knows what about them, and why their information may be shared.

What personal information do we collect and why?

P2P only obtains and retains information to enable them to provide quality support to participants and to improve their service delivery, or that which is required by their reporting bodies.

P2P collect information to:

- assess Participant's eligibility for services;
- provide safe and responsive services;
- monitor the services we provide;
- improve our services and the way we run Association activities; and
- fulfil contractual and other requirements to provide non-identifying data and statistical information to government agencies.

Keeping your information safe

Participant information will be stored in a way that reasonably protects it from misuse and loss from unauthorised access, modification and disclosure. This includes ensuring P2P systems and software are compliant with privacy legislation and data storage. P2P ensures there is up to date security protocols in place.

In dealing with personal information, P2P team members will:

- only collect and store personal information that is necessary for the functioning of the organisation and its activities;
- ensure objective, detailed, accurate and up-to-date records and information are maintained to meet legal, contractual and mandatory reporting requirements and that all requests for correction are processed as soon as practicable;.
- only collect and store sensitive information that is needed to deliver appropriate supports to a person. Sensitive information will be handled within the requirements of the Privacy Act.
- keep a participant's NDIS status and NDIS plan private. Coordinators will only share portions of a person's NDIS plan or goals with other providers, with consent, that are required to obtain service quotes or plan services and are relevant to meeting the person's goal.

In the event of a data or privacy breach, the incident will be recorded and those impacted will be contacted as soon as practically possible, including details of rectification strategies.

The Operations Manager administers secure access to electronic records.

Disclosure of Personal Information

P2P will not disclose such personal information to a third party:

- without the individual's consent; or
- unless that disclosure is required or authorised by or under law; or
- by using descriptions of individuals or details of particular situations which may inadvertently identify a person, even if they are not named. This is particularly important in small close knit communities.

There may be times where P2P is required to disclose Participant's personal information to a third party. These are the only circumstances in which this could happen:

- to prevent or lessen a serious and imminent threat to the life or health of the Participant or another person;
- provide to outside agencies with participants or participant representative's permission;
- with written consent from a person with lawful authority; or
- when required by law, or to fulfil legislative obligations such as mandatory reporting.

Requesting personal information

Information held on file can be formally requested in writing or directly via a team member who will be required to forward the request to senior management for approval. In some circumstances access to personal information may be denied. There may be real concerns that access to certain information could pose a serious threat to the life, health or safety of an individual, or to public health or public safety or have an unreasonable impact on the privacy of other people. The Operations Manager will consider all the circumstances before making this decision. Where access to information is not provided, the Operations Manager will provide a formal response explaining why access has been denied.

Complaints about perceived or suspected breaches of privacy will be addressed in line with the Feedback and Complaints Policy.

Online marketing tools and third party information and privacy

P2P uses online software to manage their communication and marketing. This may include website analytics, email campaigns and social media. The following two links detail how these third party sites collect and use information.

Google Analytics (for website) https://support.google.com/analytics/answer/6004245?hl=en
Mailchimp (for emails) https://mailchimp.com/legal/privacy/#3._Privacy_for_Contacts

P2P will not use information collected in the process of delivering services to market content to Participants without their consent.

Definitions

Confidential Information: refers to any information or document that a business or individual wishes to not make public. It can include anything that has been acquired by or made available to an individual or other legal entity in the course of the relationship between the parties.
Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

1. whether the information or opinion is true or not; and
2. whether the information or opinion is recorded in a material form or not.

Sensitive information: has a higher level of privacy protection than other personal information. It is defined in the Privacy Act to mean information or an 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;
- health information and genetic information about an individual that is not otherwise health related;
- sexual preferences or practices; or
- criminal record.

Related resources

Feedback and Complaints Policy and resources

Related legislation and policy

- Privacy Act (1988)
- QLD Information Privacy Act 2009
- Privacy Principles
- Telecommunications (Interceptions and Access) Act 1979 (Cth)
- United Nations Convention on The Rights of Persons with Disabilities
- National Standards for Disability Services
- National Disability Insurance Scheme Quality and Safeguarding Framework

Consultation & Approval

P2P staff, board, and people with a lived experience (The Sounding Board) were consulted in the development of this policy. This policy has been approved for the Operations Manager to implement.