Privacy & Confidentiality Policy

Policy 25

This policy ensures we protect and handle personal information in accordance with the NDIS and relevant privacy legislation. This policy can apply to various stakeholders including clients, ICJP team members, suppliers and visitors. We acknowledge an individual's right to privacy while recognising that personal information is required to be collected, maintained and administered in order to provide a safe working environment and a high standard of quality.

The information we collect is used to provide services to participants in a safe and healthy environment with individual requirements, to meet duty of care obligations, to initiate appropriate referrals, and to conduct business activities to support those services.

Definitions

Personal information

Personal information includes (regardless of its accuracy):

- Name, address, phone number, email address and date of birth
- Recorded opinions or notes about someone
- Any other information that could be used to identify someone.

Sensitive personal information

Sensitive personal information can include personal information that is normally private such as:

- health information
- Medicare details
- Private Health Insurance information
- bank account details
- superannuation fund details
- ethnicity
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexuality
- criminal record
- biometric information (such as fingerprints).

Data breach

An incident where personal and/or sensitive information has been accidentally or deliberately accessed and/or disclosed in an unauthorised fashion. Some common examples of data breaches include:

- Personal information accidentally mailed or emailed to the wrong recipients
- A locked filing cabinet containing personal files is broken into or left unlocked and accessed by unauthorised persons
- A computer or storage device used to store personal information is compromised as a result of a security breach, malware or poor security practices
- Personal information in printed form or on an insecure storage device is left in a public place
- Personal information accidentally or deliberately shared on social media

Where the people affected by the data breach are at risk of serious harm as a result of the breach, the incident is reportable to the Office of the Australian Information Commissioner.

Who this policy applies to

This policy applies to all representatives of I Can Jump Puddles, including key management personnel, full-time, part-time or casual staff, as well as contractors and volunteers.

This policy applies to all personal information, including sensitive personal information, used and held by the organisation for participants and employees. It also applies to all company confidential information; that is any information not publicly available.

Policy

Privacy and confidentiality commitment

- We are fully committed to complying with the privacy requirements of the Privacy Act 1988, the Australian Privacy Principles and Privacy Amendment (Notifiable Data Breaches) Act 2017 as required by organisations providing disability services
- We are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework
- We provide all individuals with access to information about the privacy of their personal information
- Individuals have the right to request access to their personal records by requesting this with their I Can Jump Puddles contact person
- Where we are required to report to government funding bodies, information provided is de-identified and relates only to services and support hours provided, age, disability, language spoken and nationality

- Personal information will only be used by us and will not be shared outside the organisation without your permission unless required by law (e.g. reporting assault, abuse, neglect, or where a court order is issued).

Security of information

- We take reasonable steps to protect the personal information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.
- Personal information is accessible to the participant and able for use by relevant ICJP employees and contractors.
- Security for personal information includes use of secure data centres, password protection for IT systems, locked filing cabinets and physical access restrictions with only authorised personnel access.
- Personal information no longer required is securely destroyed or de-identified.

Who we share personal information with

In order to provide our services to our clients, we need to share your information with various third parties:

- We will seek your consent to share your information with relevant third parties at the commencement of the service relationship.
- We will seek information about who we may need to share your personal information with at the commencement of the service relationship.
- Only that information which is relevant to the delivery of a service or support will be shared with the third party.
- Where a third party becomes relevant after the service relationship has commenced, we will seek your consent to share information with them prior to releasing any information.
- The reasons for sharing your personal information with a third party may include, but are not limited to:
    - Referring you for a service or support
    - Seeking a professional opinion about your services or support needs
    - Providing information to a funding body to assist their decision-making processes for your services and supports
    - Providing information to a plan management provider to facilitate payment for a service, support or product
    - Taking action against an outstanding debt that has not been settled in a timely manner; in this instance personal information will be limited to name, address, contact numbers and details of the outstanding debt.
    - Where we are required by legislation or statutory obligation to provide specific information, such as reporting report, abuse or neglect, or where a court order is issued.
- The vendor of our client record management system has access to personal information as there are certain technical aspects of this system that need to be outsourced; this third party provider is also bound by the Australian Privacy Principles.

- Your personal information will not be provided to any third party for the purposes of direct marketing.

Data breaches

- We will take reasonable steps to reduce the likelihood of a data breach occurring, including by storing personal information securely and making it accessible only by relevant employees and contractors.
- If we know or suspect your personal information has been accessed by unauthorised parties and we think this could cause you harm, we will take reasonable steps to reduce the chance of harm and advise you of the breach.
- Where necessary, we will notify the Office of the Australian Information Commissioner of a data breach.

Breach of privacy and confidentiality

- A breach of privacy and confidentiality will be managed as an incident, in line with the I Can Jump Puddles Incident Management Policy and Procedure.
- A data breach, or suspected data breach, will be managed in accordance with the ICJP Data Breach Procedure.
- An intentional breach of privacy and confidentiality may result in disciplinary action up to and including termination of employment.

Related Documentation

- I Can Jump Puddles Information Security Policy
- I Can Jump Puddles Incident Management Policy
- I Can Jump Puddles Data Breach Procedure
- I Can Jump Puddles Incident Management Procedure
- I Can Jump Puddles Records Management Procedure
- I Can Jump Puddles Information Sharing Guidelines – Appendix
- I Can Jump Puddles Consent to Share Information Form