

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 finger prints).

Data breach

A data breach is type of security incident where personal, sensitive or confidential information normally protected, is deliberately or mistakenly copied, sent, viewed, stolen or used by an unauthorised person or parties. A data breach where people affected by the data breach are at risk of serious harm as a result, is reportable to the Office of the Australian Information Commissioner. ICJP has a separate Data Breach Response Policy & Plan that is available to all team members.

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 non-identifiable and related to services and support hours provided, age, disability, language, 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 is able for use by relevant workers
- 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 permitted access
- Personal information no longer required is securely destroyed or de-identified.

Who we share personal information with

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

- Some team members at I Can Jump Puddles are not employed by the organisation, they are their own entities, and therefore legally your personal information is shared by these parties. It is necessary for our team members to share information with each other to provide cover for leave, as well as to collaborate on management of clients, therefore all team members operating under the I Can Jump Puddles banner have access to all I Can Jump Puddles clients' personal details.
- Personal information is shared, with your consent, with other external providers to whom referrals are made.
- The vendor of our client 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.
- Our client database uses a Salesforce platform, stored on a server that is located overseas; specifically, the server is located in Kobe, Japan. The Act on the Protection of Personal Information ("APPI") regulates privacy protection issues in Japan and the Personal Information Protection Commission (the "PPC"), a central agency acts as a supervisory governmental organisation on issues of privacy protection. All reasonable steps have been taken to ensure storage of data with Salesforce in Japan meets Australian privacy legislation requirements. In addition, Salesforce complies with the ASP/SaaS Information Disclosure Certification System for organisations in Japan. It also complies with ISO standards 27001 (Compliance with specific information security and risk management requirements), 27101 (Adherence with ISO/IEC 27002 Code of Practice controls for cloud services) and 27018 (Adherence with Code of Practice controls for protection of personal information). All information being sent to and from the server based in Japan uses appropriate encryption.
- Staff, contractor and supplier details are stored on Google Drive, a cloud-based service with the server located in Sydney, Australia.
- Personal information is shared with the NDIA and various plan managers in order to receive payment for provision of services.
- Personal information limited to name, address, contact numbers and details of outstanding debt may be shared with debt collection agencies should outstanding debts not be settled in a timely manner.

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 storing personal information securely and accessible only by relevant workers
- 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, and if necessary, the Office of the Australian Information Commissioner.

Breach of privacy and confidentiality

- A breach of privacy and confidentiality is an incident – follow the I Can Jump Puddles Incident Management Policy and Procedure to resolve.
- A data breach, or suspected data breach, should be managed in accordance with the ICJP Data Breach Response Policy & Plan.
- An intentional breach of privacy and confidentiality will result in disciplinary action up to and including termination of employment.

Related Documentation

- I Can Jump Puddles Information Security Policy
- I Can Jump Puddles Data Breach Response Policy & Plan
- I Can Jump Puddles Incident Management Policy
- I Can Jump Puddles Incident Management Procedure
- NDIS (Provider Registration and Practice Standards) Rules 2018
- I Can Jump Puddles Consent to Share Information Form