


Privacy			Policy and Procedure
Document name	Privacy	CEO approved	
Category	Organisational Governance		
Version	1	Approval date	August 2025
Implementation date	31 August 2025	Review date	August 2028

Purpose

To set out how we collect, use, disclose, store and secure personal information of participants and workers. The policy and procedure outlines how Identitywa Disability Services Limited (Identitywa) upholds the right to privacy of participants and workers.

It guides Identitywa workers on how to manage private information, records in hard copy or electronic versions to ensure legal obligations are met.

Who is this policy and procedure for?

This Policy and Procedure applies to all Identitywa workers and participants.

Policy statement

Identitywa complies with the Privacy Act 1988 and applies the [Australian Privacy Principles](#) (APP) while collecting, storing and using personal confidential information of participants and workers for the purpose of delivering high quality services.

Identitywa is committed to safeguarding personal information that is provided and ensuring that this information is managed appropriately and only used for its intended purpose.

When in possession of records containing personal information, Identitywa will ensure that:

- Consent is given for the collection of personal information
- Workers and participants know what information and records are collected.
- Records are protected against loss, unauthorised access and/or modification.
- Unauthorised use or disclosure of personal records and/or information is prevented.
- Information is used and disclosed for the purpose given at the time it is collected.

Principles

Identitywa collects personal and sensitive information of participants as required to deliver the requested services. It is important for the information received to be as accurate and complete as possible. This information can include, but is not limited to, medical reports and records, specialist behaviour support plans, participant support and safety plans, and other documents and records as required.

Personal information includes a person's name, address, contact details (e.g., phone number or email) and date and place of birth. Sensitive information may include sexuality, race, religion, and health information. Information collected may come from a variety of sources and include medical and allied health reports and records.

Australian Privacy Principles

Identitywa complies with the [Australian Privacy Principles](#) (APP). These principles establish the obligations in relation to handling, holding, accessing, and correcting personal information. Following are the statements addressing the APP:

Open and Transparent Management of Personal Information

- Information will be retained as per Identitywa's *Record Management and Archive Policy and Procedure*.
- Information is collected from a variety of sources and may include participants, carers, advocates, and other third parties such as Government agencies and medical practitioners.
- All Identitywa's processes are transparent, and policies and procedures are accessible for workers on staff portal or can be requested at any time.

Anonymity and Pseudonymity

It is noted that a person may prefer to remain anonymous when dealing with Identitywa. For example, a member of the public may make an inquiry into Identitywa's service without providing any of their details. A pseudonym may also be used in place of a person's actual name.

Collection of Solicited Personal Information

Personal and sensitive information must only be collected for the purpose of providing a service for the participant. Information collected includes information about personal circumstances, information about identity, and records relating to health.

Dealing with Unsolicited Personal Information

Unsolicited information will not be used by Identitywa and if appropriate, will be destroyed or de-identified.

Notification of the Collection of Personal Information

All participants sign Consent forms at commencement with the organisation. This includes consent to obtain information and to share information with third parties.

Use or Disclosure of Personal Information

Identitywa will not disclose information about participants or workers without obtaining consent. The only exception applies if directed by an Australian law or court/tribunal order.

Direct Marketing

Identitywa will not share information about participants or workers for direct marketing, unless the participant or worker has given consent. Participants or workers will have the option to "opt out" of any marketing activities.

Cross-border Disclosure of Personal Information

All Identitywa servers are based in Australia. No data is sent offshore. If a provider of servers discloses their offshore connection, Identitywa must determine if the provider meets Australian Privacy standards before a contract is committed.

Adoption, Use or Disclosure of Government Related Identifiers

Identitywa will not use Government identifiers for participants of the service, unless there is an exemption as per the APP.

Quality of Personal Information

Identitywa takes all reasonable steps to ensure the personal information collected, used, or disclosed is accurate, complete, and up to date.

Security of Personal Information

When in possession or control of a record containing personal information, Identitywa takes all reasonable steps to ensure that the record is protected against loss, unauthorised access, modification, or disclosure.

Access to Personal Information

- Should participants or workers request to view their own personal information as held by Identitywa, Identitywa provides them with access as requested.
- Participants and workers will be provided access to their personal information in the format requested.

Exemptions to Granting Access to Personal Information

There are exceptions allowing Identitywa to deny access, consistent with the Privacy Act. Identitywa is not required to give a participant or worker access to their own personal information if any of the following apply:

- It is believed that granting access would pose a serious threat to the life, health, or safety to any person, or to public health or safety.
- Granting access would have an unreasonable impact on the privacy of participants or worker.
- The request for access is frivolous or vexatious.
- The personal information is part of existing or anticipated legal proceedings between the individual and Identitywa.
- Granting access would reveal the intentions of Identitywa in relation to negotiations with the participant or worker in such a way as to prejudice those negotiations.
- Granting access would be unlawful.
- Denying access is required or authorised by or under an Australian law or a court/tribunal order.
- Identitywa has reason to suspect unlawful activity or misconduct of a serious nature that relates to Identitywa's functions or activities has been, is being, or may be engaged in.
- Granting access would be likely to prejudice the taking of appropriate action in relation to suspected unlawful activity or serious misconduct.
- Granting access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
- Granting access would reveal evaluative information generated within Identitywa, in connection with a commercially sensitive decision-making process.

Correction of Personal Information

Identitywa will maintain information that is accurate, up-to-date, complete, relevant, and not misleading. Participants are entitled to have their information corrected and may request this in writing by emailing admin@identitywa.com.au.

Procedure

Dealing with personal information

In dealing with personal information, Identitywa workers will ensure privacy for participants, their support network, or workers when they are being interviewed, or when discussing matters of a personal or sensitive nature.

Roles and responsibilities

All workers are responsible for the management of personal information to which they have access to.

The Communications and Marketing Officer is responsible for content in publications, communications and website and must ensure the following:

- Appropriate consent is obtained for the inclusion of any personal information about any individual including Identitywa workers and participants
- Information being provided by other agencies or external individuals conforms to privacy principles
- That the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website.

Information requested about the Participant

There are four key elements of consent which Identitywa adheres to before releasing private information:

- The person is adequately informed prior to giving consent.
- The person gives consent voluntarily.
- The consent is current and specific.
- The person has the capacity to understand and communicate their consent.

Consent is obtained before information is collected or shared with a third party.

When a participant engages with Identitywa for services, a *Consent Form* is completed for relevant information and signed.

If a different reason for the purpose of using the information arises, the participant is notified, the need for further consent clarified and an updated Consent Form is completed.

Consent forms are reviewed at least annually and updated as required when situation, information, or consent changes.

Consent forms clearly identify who is giving consent for sharing information, for example, the participant, a family member, guardian or alternative decision maker.

Information may be made available in alternative formats such as Easy Read and access to free language interpreting services is also available upon request. Privacy information is displayed on the Identitywa website.

If information is to be used on a social network site, consent must be obtained. Similarly, Identitywa needs to secure written permission before using any images or videos of participants.

For further information please refer to the Consent Policy and Procedure.

Request for information by workers or ex-workers

Current workers can access their private information held by Identitywa on the electronic HR system, Employee Connect.

Former workers who want to access their private information held by Identitywa, need to contact the HR team to have their information released to them. Ex- workers need to provide identification, including their Australian tax file number (TFN), before any information can be released.

Security of Participants Records

All workers are responsible for ensuring the security of devices provided to them by Identitywa for their role (e.g., laptops, phones). All provided devices are password protected. All electronic records have specific levels of security access to ensure only authorised workers have access to private information held on a need-to-know basis.

Identitywa's information and communication technology systems are secured with installed firewalls, access and password protection, and in parts multi-factor authentication.

Information is held in both paper-based and electronic mediums. Hard copy records are kept in locked cabinets and/or in a secure room. All devices are password protected. Archived documents which exceed retention timeframes are securely destroyed.

Personal information is destroyed by secure methods as per the *Record Management and Archiving Policy and Procedure*, if it is no longer needed for the purpose for which it was intended, unless retention is required by law.

Identitywa premises are locked with a monitored security system in place after hours.

Human Resource Records

Information collected from potential and current workers of Identitywa include information from third parties such as referees, license checks, and registration. Workers' personal records are kept confidential, and access is limited to authorised persons only.

The Australian Privacy Principles do apply to personal information including about unsuccessful job candidates. This can include applicant's resumes, contact details, references and academic transcripts.

Third parties providing recruitment, training, human resources, payroll or other services to Identitywa under a contract may need to comply with the Australian Privacy Principles.

Compliance

All Identitywa workers have a responsibility to report any breach or suspected breach of privacy to management. Failure to comply with this policy may lead to disciplinary action including potential termination of employment.

All Identitywa workers must read and understand this policy upon employment. They are also required to attend the Code of Conduct session and sign the Code of Conduct as well as the confidentiality agreement at commencement of employment.

Notifiable Data Breach

Identitywa is required to notify affected individuals and the Commissioner of eligible data breaches as per the Privacy Act 1988 (Cth), as amended by the Privacy Amendment (Notifiable Data Breaches) Act 2017. Please refer to the Data Breach Policy and Procedure for more information.

Accessibility

If you are a participant and speak a language other than English and you need an interpreter, you can contact the Translating and Interpreting Service (TIS) for free translation services. Dial 131 450 and ask your interpreter to call (08) 9474 3303 for you.

If you're deaf or find it hard to hear or speak to hearing people on the phone, call the National Relay Services (NRS) TTY 133 677.

How do we know we are getting it right?

This document is reviewed within the framework of Identitywa's quality assurance and continuous improvement process, in consultation with key stakeholders. Process performance and effectiveness are measured against Identitywa's standards, objectives, and practices as part of a scheduled review of this and other related documents based on the level of risk to participants and the organisation.

All Identitywa policies and procedures are measured against the NDIS Practice Standards and other applicable standards, such as the National Catholic Safeguarding Standards.

Definitions

Participant

A person supported by Identitywa, such as a client, resident, or other recipient of services.

Support Network

Family, friends, carers, and other people who have a supportive relationship with a participant.

Personal Information - Privacy Act 1988 (Cth).

'Information or an opinion about an identified individual, or an individual who is 'reasonably identifiable':

- a. whether the information or opinion is true or not; and
- b. whether the information or opinion is recorded in a material form or not.'

Sensitive Information

Information or an opinion about an individual's membership of a professional or trade association or criminal record. Sensitive information also includes health information and genetic information about an individual that is not otherwise health information – Privacy Act 1988 (Cth).

Worker

A person who carries out work in any capacity for a person conducting a business, including work as:

- An employee
- A contractor or sub-contractor/sole trader
- An employee of a contractor or sub-contractor or sole trader
- A student, trainee, apprentice, volunteer, or host.

The legal and regulatory requirements we have to follow[Australian Human Rights Commission Act 1986](#)[Australian Privacy Principles](#)[Better Care, Better Services Standards](#)[Fair Work Act 2009](#)[Guardianship and Administration Act 1990](#)[National Catholic Safeguarding Standards](#)[National Disability Insurance Scheme \(NDIS\) Act 2013](#)[NDIS Code of Conduct](#)[NDIS \(Incident Management and Reportable Incidents\) Rules 2018](#)[NDIS \(Complaints Management and Resolution\) Rules 2018](#)[NDIS Practice Standards and Quality Indicators](#)[NDIS \(Provider Registration and Practice Standards\) Rules 2018](#)[NDIS \(Quality Indicators\) Guidelines 2018](#)[NDIS \(Specialist Disability Accommodation\) Rules 2021](#)[Privacy Amendment \(Notifiable Data Breaches\) Act 2017](#)[State Records Act 2000](#)[The Privacy Act 1988 \(Cth\)](#)[The State Administrative Tribunal \(SAT\) Act 2004](#)[Work Health and Safety Act 2020](#)[Work Health and Safety Regulations \(General\) 2022](#)**Other related documents**

Application for Access to Personal Information

Confidentiality Agreement – External Parties

Consent Policy and Procedure

Data Breach Policy and Procedure

Identitywa Code of Conduct

Social Media - Personal Use Policy

Social Media - Official Use Policy and Procedure

Duty of Care Policy

Complaints and Feedback Policy and Procedure

Record Management and Archiving Policy and Procedure

Further Information:

[Australian Privacy Principles Guidelines](#)[Fair Work Ombudsman – Workplace Privacy Best Practice Guide](#)**Do you need to know more?**

If you have any questions regarding policies, procedures, and reviews or if you would like to be involved in our policy development program, please contact the Quality and Compliance Team on (08) 9474 3303.