ABOVE & BEYOND DISABILITY SOLUTIONS

# Privacy Policy and Procedure

## Policy statement

Above and Beyond Disability Solutions Pty Ltd (AABDS) is committed to protecting the privacy, dignity, confidentiality and human rights of all participants, families, carers, advocates and employees.

AABDS recognises that participants have the right to privacy and control over their personal information and will ensure all personal and sensitive information is collected, stored, accessed, used, disclosed and destroyed lawfully, securely and transparently.

## Scope

This policy applies to all employees, participants, families, advocates, contractors, volunteers or business partners. This policy is owned by the Governing Body.

## Principles

AABDS will ensure:

- participants are treated with dignity, privacy and respect;
- personal information is only collected where reasonably necessary for service delivery, legal obligations or organisational operations;
- participants are informed about why information is collected, how it will be used, who it may be shared with, and how it will be protected;
- information is collected lawfully, fairly and directly from the participant wherever practicable;
- informed consent is obtained before collecting, using or disclosing personal information unless otherwise authorised or required by law;
- participants may withdraw or amend consent at any time;
- information is accurate, complete, current and relevant;
- participants can access and correct their information;
- privacy information is available in accessible formats, including Easy Read, electronic and translated formats where reasonably practicable;
- participants are supported to understand their privacy rights using their preferred communication methods;
- confidentiality is maintained during all verbal, written, electronic and face-to-face interactions;
- secure systems are used to protect records and communications;
- all workers receive training regarding privacy, confidentiality, cyber security and mandatory reporting obligations;
- all actual or suspected privacy breaches are responded to promptly; and
- all recordkeeping complies with legal retention and destruction requirements.

## Practice requirements

AABDS is committed to maintaining systems that protect information from misuse, interference, loss, unauthorised access, modification or disclosure, including information held electronically, verbally, visually and in hard copy.

## Collection

AABDS may collect personal and sensitive information including:

- participant names and contact details;
- date of birth;
- emergency contacts;
- medical and health information;
- disability and support needs;
- behavioural or risk information;
- cultural, communication and accessibility requirements;
- guardianship or decision-making arrangements;
- service agreements and support records;
- billing information;
- incident and complaint records; and
- audio, photographic or video recordings where consent has been obtained.

Information will only be collected where it is:

- reasonably necessary for delivering supports and services;
- required under law;
- necessary to protect health, safety or wellbeing; or
- required for incident reporting, safeguarding or regulatory obligations.

Where lawful and practicable, participants may choose to use a pseudonym or remain anonymous.

## Consent

AABDS will obtain informed consent before collecting, using or sharing personal information unless:

- disclosure is required or authorised by law;
- there is a serious threat to life, health or safety;
- mandatory reporting obligations apply;
- a reportable incident must be notified to the NDIS Commission, police or another authority;
- information is required during legal proceedings or investigations.

Consent processes must:

- be voluntary and informed;
- use accessible communication methods;
- consider supported decision-making arrangements;
- be documented and securely stored; and
- allow participants to withdraw consent at any time.

## Use and disclosure of information

AABDS will only use or disclose personal information:

- for the primary purpose for which it was collected;
- for directly related purposes reasonably expected by the participant;
- with participant consent; or
- where otherwise required or authorised by law.

Information may be disclosed to:

- the NDIA;
- the NDIS Quality and Safeguards Commission;
- health professionals;
- emergency services;
- guardians or nominees;
- advocates authorised by the participant;
- courts, tribunals or law enforcement agencies; or
- other providers involved in participant supports.

AABDS will not sell participant information or use personal information for direct marketing purposes.

AABDS does not routinely disclose personal information overseas. If overseas disclosure becomes necessary, participants will be informed and appropriate safeguards will be implemented.

## Storage and Security

AABDS will implement reasonable physical, administrative and technological safeguards to protect information, including:

- password-protected systems;
- secure cloud storage and encryption;
- restricted access permissions;
- locked filing systems;
- secure disposal and shredding practices;
- multi-factor authentication where practicable;
- cyber security controls and monitoring;

- confidentiality agreements for employees and contractors,
- staff privacy training.

All electronic communications containing sensitive or personal information must be transmitted securely.

## Access and Correction

Participants may request access to their personal information or request corrections to inaccurate, incomplete or outdated information. Requests will generally be responded to within 14 business days.

Access may be refused only where permitted under legislation, including where:

- access would pose a serious threat to health or safety;
- access would unreasonably impact another person's privacy;
- the request is frivolous or vexatious;
- legal proceedings apply;
- access would be unlawful; or
- refusal is otherwise authorised by law.

If access is refused, AABDS will provide written reasons where appropriate and information regarding complaints processes.

## Privacy Breaches and Data Breaches

AABDS will respond promptly to all actual or suspected privacy breaches. Responses may include:

- immediate containment actions;
- risk assessment;
- participant notification;
- mandatory reporting;
- investigation and corrective action;
- review of systems and practices; and
- notification under the Notifiable Data Breaches scheme where required.

Serious breaches may also require notification to the NDIS Commission, police or other regulatory authorities.

## Maintaining Dignity and Confidentiality

Employees must respect participant dignity and privacy during all supports and interactions, including:

- respecting personal space and boundaries;
- maintaining privacy during personal care;
- seeking consent before physical contact;
- conducting discussions confidentially;

- protecting participant information from being overheard or viewed by others; and
- ensuring private environments for personal care and communication.

## Record Retention and Disposal

AABDS will retain records in accordance with legislative and operational requirements. When records are no longer required, they will be securely destroyed or de-identified in a manner that protects confidentiality.

## Artificial Intelligence (AI) and Digital Technologies

AABDS recognises that AI, automation and digital technologies may be used to support administrative, operational and service delivery functions. AABDS is committed to ensuring all use of AI aligns with participant rights, privacy obligations, ethical practice and human rights principles.

AABDS will ensure:

- AI technologies are used lawfully, ethically, safely and transparently;
- AI does not replace human decision-making in matters involving participant safety, rights, safeguarding, restrictive practices, complaints, incident management or clinical judgement;
- participants are informed where AI tools may be used to assist with administrative functions, communication, documentation or service improvement activities;
- personal and sensitive information will not be entered into AI systems;
- AI-generated information is reviewed by appropriately authorised employees before being relied upon, distributed or included in participant records;
- employees using AI tools must read and understand AABDS's AI Use policy that clearly outlines privacy, confidentiality, ethical use and information security;
- AI systems are monitored to minimise risks relating to bias, discrimination, misinformation, inaccurate outputs or breaches of participant rights;
- participants maintain the right to ask questions about how their information is used in AI-supported processes; and
- all AI use supports participant dignity, choice, control, inclusion and human rights.

AABDS prohibits the use of AI technologies to:

- unlawfully disclose confidential information;
- make automated decisions that significantly affect participant rights or supports without human oversight;
- create misleading, discriminatory or harmful content;
- replace mandatory professional judgement or safeguarding responsibilities; or
- record or monitor participants without lawful authority and informed consent.

Any actual or suspected data breach, privacy breach or inappropriate AI use must be reported immediately in accordance with AABDS's Incident Management, AI Use and Privacy policies.

## Complaints

Participants and stakeholders may make complaints regarding privacy or confidentiality concerns without fear of disadvantage or retaliation.

Complaints may be made verbally, in writing or through an advocate.

All complaints will be managed in accordance with the Complaints Management policy and relevant legislative requirements.

Participants may also lodge complaints with the Office of the Australian Information Commissioner (OAIC); or the NDIS Quality and Safeguards Commission.

## Related policies

- Code of Conduct policy
- Choice & Control policy
- AI Use policy
- Promoting and Protecting Rights policy
- Preventing Abuse, Neglect and Exploitation policy
- Complaints Management policy
- Incident Management policy

## Related links

- the Privacy Act 1988 (Cth)
- the Australian Privacy Principles (APPs)
- the National Disability Insurance Scheme Act 2013
- the NDIS Code of Conduct
- the NDIS Practice Standards and Quality Indicators
- the NDIS (Incident Management and Reportable Incidents) Rules
- the Freedom of Information Act 1982
- the Disability Services and Inclusion Act 2023 (Qld)
- the Privacy Amendment (Notifiable Data Breaches) Act 2017

## Acknowledgements

AABDS adheres to the NDIS Code of Conduct and NDIS Practice Standards for providers and workers. Our Quality Services and Supports promote the National Standards for Disability Services – evidence Guide.

The organisation promotes the Human Rights principles of the Convention on the Rights of Persons with Disabilities.

# Privacy procedure

## Purpose

The purpose of this procedure is to establish clear standards and processes for protecting the privacy, dignity, confidentiality and personal information of all participants engaged with Above and Beyond Disability Solutions Pty Ltd (AABDS).

This procedure supports AABDS to comply with applicable Commonwealth and State legislation, the NDIS Practice Standards and the organisation's commitment to participant rights, safeguarding and ethical service delivery.

## Scope

This procedure applies to all employees, participants, families, advocates, contractors, volunteers or business partners. This policy is owned by the Governing Body.

## Principles

AABDS will ensure:

- participant information is handled lawfully, fairly and transparently;
- only information reasonably necessary for service delivery or legal obligations is collected;
- participants are informed about how their information is collected, stored, used and disclosed;
- participants are supported to understand and exercise their privacy rights;
- informed consent is obtained wherever required;
- confidential information is protected against misuse, loss, unauthorised access or disclosure;
- records are securely maintained and disposed of appropriately;
- employees understand their privacy obligations;
- privacy breaches and data breaches are responded to immediately; and
- all privacy practices uphold participant dignity, choice, control and human rights.

The following procedures are to be implemented to ensure AABDS and its employees meets its policy objective to ensure all participants have the same level of privacy and confidentiality as is expected by the rest of the community.

## Collection of information

AABDS will:

- only collect information directly relevant to service delivery, participant safety and wellbeing, duty of care obligations, funding and reporting requirements, and legal or regulatory obligations.
- collect information directly from the participant wherever practicable;

- explain to participants:
  - why information is required;
  - how it will be used;
  - who it may be shared with;
  - how it will be stored and protected;
  - how they can access or correct information; and
  - how complaints can be made;
- obtain informed consent before collecting information from third parties unless otherwise authorised by law;
- provide privacy information in accessible formats and communication methods suitable to participant needs;
- ensure participants can involve advocates, nominees, guardians or supported decision-makers where appropriate; and
- minimise collection of sensitive information wherever practicable.

## Consent

Before information is shared or obtained from external sources, AABDS employees must:

- obtain documented informed consent;
- ensure the participant understands what information will be shared, why it is being shared, who will receive it, and any associated risks.
- document consent within participant records;
- recognise that consent may be withdrawn at any time.

Consent is not required where disclosure is:

- required by law;
- necessary to prevent serious harm;
- related to mandatory reporting obligations;
- required for reportable incidents;
- authorised by a court or tribunal; or
- permitted under privacy legislation.

## Use and disclosure of information

AABDS will only use or disclose personal information:

- for the primary purpose it was collected;
- for directly related purposes reasonably expected by the participant;
- with participant consent; or
- where otherwise authorised or required by law.

Information may be disclosed to:

- the NDIA;
- NDIS Quality and Safeguards Commission;
- health professionals;
- emergency services;
- guardians, nominees or advocates;
- law enforcement agencies;
- courts or tribunals; and
- other providers involved in participant supports.

AABDS will not sell personal information or use participant information for direct marketing purposes.

## Storage and security of information

AABDS will ensure:

- participant files are securely stored;
- paper records are kept in locked cabinets or secure locations;
- electronic records are password protected and access restricted;
- systems use appropriate cyber security protections;
- only authorised employees access participant information;
- records are not left unattended or visible to unauthorised persons;
- identifying information is not displayed publicly;
- secure disposal methods are used for confidential documents;
- portable devices are protected and encrypted where practicable; and
- electronic communications containing sensitive information are transmitted securely.

All employees must immediately report suspected security risks or breaches.

## Access and correction requests

Participants, families, carers or authorised representatives may request access to participant information.

AABDS will:

- respond to requests within 14 business days where practicable;
- verify the identity and authority of the requester;
- provide access in accessible formats where required; and
- correct inaccurate, incomplete or outdated information.

Access may be refused only where permitted by legislation. Where access is refused, written reasons and complaint options will be provided.

## Maintaining privacy and dignity during service delivery

Employees must protect participant dignity by:

- respecting personal boundaries and privacy;
- obtaining consent before physical contact;
- conducting confidential discussions privately;
- ensuring privacy during personal care;
- maintaining confidentiality during transport and community access;
- protecting verbal and written information from being overheard or viewed; and
- using respectful, person-centred communication.

## Photographs, video and audio recordings

AABDS will not photograph, video record, audio record, or publicly display participant images or recordings without documented informed consent unless otherwise authorised by law.

Consent forms must specify how recordings will be used, where they may appear, who may access them, and how consent can be withdrawn.

## Data breaches management

A data breach is an unauthorised access or disclosure of personal information, or loss of personal information, including:

- unauthorised access to information;
- unauthorised disclosure;
- loss of records or devices;
- hacking or cyber incidents;
- accidental disclosure; or
- misuse of participant information.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

- lost USB devices or laptops;
- unauthorised employee access;
- phishing or cyber attacks;
- stolen documents; or
- disclosure of information without consent.

If AABDS is subject to a data breach, the organisation will undertake the following steps:

## 1. Identify

AABDS Management will:

- assess whether a breach has occurred;
- determine:
  - what information was involved;
  - who is affected;
  - whether the breach is ongoing;
  - the level of risk or harm;
  - whether mandatory reporting applies; and
  - what immediate action is required;
- preserve evidence; and
- document all actions taken.

## 2. Contain

AABDS will take immediate steps to:

- stop unauthorised access or disclosure;
- isolate affected systems;
- disable compromised accounts;
- recover information where possible;
- engage IT specialists if required; and
- reduce risks to affected individuals.

## 3. Assess

Management will assess:

- likelihood of serious harm;
- sensitivity of the information;
- whether information is recoverable;
- who has obtained access; and
- whether notification obligations apply.

## 4. Notify

Where required under the Notifiable Data Breaches Scheme or other legislation, AABDS will notify:

- affected individuals;

- the Office of the Australian Information Commissioner (OAIC);
- the NDIS Commission;
- police or other authorities where necessary; and
- other relevant stakeholders.

Notifications will include:

- the nature of the breach;
- information affected;
- actions taken;
- recommendations for affected individuals; and
- contact details for support or further information.

## 5. Review and Improve

Following a breach, AABDS will:

- investigate contributing factors;
- review systems and procedures;
- implement corrective actions;
- provide additional employee training;
- strengthen cyber security controls; and
- monitor for recurrence.

## Responsibility

## Employees

Employees are responsible for:

- maintaining confidentiality;
- securely handling participant information;
- complying with this procedure;
- reporting suspected breaches immediately;
- using approved communication and storage systems only; and
- completing mandatory privacy and cyber security training.

## Managers

Managers are responsible for:

- monitoring compliance with this procedure;

- supporting employees to understand obligations;
- responding to breaches and complaints;
- ensuring secure recordkeeping practices; and
- implementing corrective actions where required.

## Directors and Governing Body

Directors and the Governing Body are responsible for:

- governance oversight;
- monitoring compliance systems;
- ensuring adequate resources and training;
- reviewing privacy risks;
- monitoring legislative compliance; and
- supporting continuous improvement.

## Reporting

All privacy breaches, confidentiality concerns, data breaches, complaints, and unauthorised disclosures must be documented within the organisation's incident, complaints or risk management systems.

Serious matters will be escalated in accordance with legislative and NDIS reporting obligations.

## Review and Continuous Improvement

AABDS will regularly review privacy incidents, complaints, data breaches, participant feedback, cyber security risks, legislative updates, and audit findings to identify opportunities for continuous improvement.

This procedure will be reviewed at least annually or following significant legislative, operational or privacy changes.

## Key contact

Questions about how to implement this procedure should be directed to Kristy McPherson, Director on 0417 069 124.

## DOCUMENT HISTORY

| | | | |
|---|---|---|---|
| **Policy name** | Privacy | **Policy owners** | Governing Body |
| **Policy created** | July 2018 | **Approved by Board** | Oct 2018 |
| **Policy reviewed** | July 2019 | **Approved by Board** | July 2019 |
| **Policy reviewed** | Oct 2019 | **Approved by Board** | Oct 2019 |
| **Policy reviewed** | Aug 2021 | **Approved by Board** | Aug 2021 |
| **Policy reviewed** | Dec 2022 | **Approved by Board** | Dec 2022 |
| **Policy reviewed** | Feb 2024 | **Approved by Board** | Feb 2024 |
| **Policy reviewed** | May 2026 | **Approved by Board** | May 2026 |
| **Current version no.** | 5 | **Due for review** | May 2028 |