Privacy policy

Policy statement

Above and Beyond Disability Solutions Pty Ltd (AABDS) is committed to ensuring that all participants have the same level of privacy and confidentiality as is expected by the rest of the community.

Scope

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

Principles

- Consistent processes and practices are in place that respect and protect the personal privacy and dignity of each participant.
- Each participant is advised of confidentiality policies using the language, mode of communication and terms that the participant is most likely to understand.
- Each participant understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.
- AABDS ensures the organisation and its employees will always manage participant's personal information in an open and transparent way.
- AABDS will ensure its Privacy policy is maintained and kept up to date to align with all necessary State and Federal legislation.
- AABDS will ensure the Privacy policy is readily available to all participants, their families, carers or advocates in numerous forms to meet the needs of all stakeholders, including hard copy, easy reads and electronic versions on the organisation's website.
- If a participant, their family, carer or advocate requests a copy of the organisation's Privacy policy in a particular form, AABDS will take such steps as are reasonable in the circumstances to give the participant a copy in that form.
- All participants have the option of not identifying themselves, or of using a pseudonym, when dealing with AABDS in relation to a particular matter, unless it is impracticable for AABDS to deal with individuals who have not identified themselves or who have used a pseudonym.
- AABDS can only collect participant information if the participant, their family, carer or advocate consents to the collection of the information and it's reasonably necessary for, or directly related to, one or more of the organisation's functions or activities.
- Participant information that was collected for a particular purpose (the primary purpose) will not be disclosed by AABDS for any other purpose unless the participant, their family, carer or advocate has consented to the use or disclosure of the information or the

participant would reasonably expect AABDS to use or disclose the information for the alternative purpose.

- AABDS will not use any participant information for the purpose of direct marketing.
- AABDS will take such steps to ensure that the personal information is accurate, up-to-date and complete.
- AABDS will ensure participant information is protected from misuse, interference and loss; and from unauthorised access, modification or disclosure.
- AABDS ensures participant information is readily available to them on request by the participant, their family, carer or advocate unless:
    - the organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
    - giving access would have an unreasonable impact on the privacy of other individuals;
    - the request for access is frivolous or vexatious;
    - the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings;
    - giving access would be unlawful; or
    - denying access is required or authorised by, or under, an Australian law or a court/tribunal order.
- AABDS will respond to all requests for access to the personal information within 14 days after the request is made.
- If AABDS believes any participant information is inaccurate, out of date, incomplete, irrelevant or misleading, the organisation will take the necessary steps to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Practice requirements

- **Collection**
    - If collecting from someone other than the participant, or the participant is not aware of the collection, AABDS will include facts an circumstances of the collection;
    - The participant is informed of the purpose of collecting the information;
    - The participant is provided with a copy of the Privacy policy, including information on the access, correction and complaints procedures;
    - AABDS will provide detais of any entity we may disclose information to;
    - AABDS will not send information overseas;

- **Privacy** - All participants have a right to privacy in relation to the collection, use and disclosure of information concerning them, and in the dignified way services are delivered to them.

- **Consent** - Participants have the right not to have their personal information disclosed to others without their informed consent. Personal information is information or an opinion about a person whose identity is reasonably identifiable from that information or opinion, E.g. a person's name, address, date of birth and details about their health or disability. Consent to share information may be changed or withdrawn by the participant at any time they choose. All request must be made in writing to maintain accurate record keeping processes.

- **Informed** – AABDS recognises that all participants should be kept informed on how their information will be used and stored. AABDS and its employees are responsible for explaining to participants:
    - the kinds of personal information that will be collected and held, including recorded audio and visual material;
    - why this information is held;
    - who will have access to this information;
    - how AABDS will keep the information secure;
    - how this information will be used;
    - how to access and amend information held about them;
    - how to make a complaint if they feel that AABDS has breached their privacy obligations.

- **Exceptions** - AABDS and its employees are obliged to be aware of situations where other legal obligations may provide an exemption to obtaining informed consent from an individual. This might include mandatory reporting requirements on child protection matters, and obligations to report incidences of violence, exploitation, neglect and abuse, and sexual misconduct to the NDIS Commission and Police.

- **Maintaining dignity** - AABDS and its employees must be aware of the privacy needs and preferences of our participants and deliver services in a way that maintains personal dignity. This includes:
    - maintaining the confidentiality of the participant's personal information;
    - requesting permission to perform, and explaining procedures that involve physical touch or the invasion of personal space;
    - the timely provision of services to prevent embarrassment and discomfort such as toilet breaks or the changing of incontinence pads;
    - considering everyday personal privacy needs such as being able to shower and dress in a private and comfortable space.

In dealing with personal information, AABDS abides by the obligations imposed under federal law, including the Privacy Act 1988. The organisation is also bound by confidentiality and secrecy provisions in the National Disability Insurance Act (2013).

Related policies

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

Related links

- Anti-Discrimination Act 1991 (Qld)
- Disability Discrimination Act (1992)
- Information Privacy Act 2009
- A New Tax System (Goods and Service Tax) Act 1999
- Freedom of Information Act 1982, Privacy Act 1988
- Australian Privacy Principles
- National Disability Insurance Scheme Act 2013
- National Disability Insurance Scheme (Protection and Disclosure of Information) Rules 2013
- National Disability Insurance Scheme (Procedural Fairness) Guidelines 2018
- Privacy Act 1988
- Archives Act 1983
- Australian Privacy Principles

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.

POLICY 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
Current version no.	3	Due for review	Feb 2024

Privacy procedure

The purpose of this procedure is to establish standards of privacy and confidentiality in Above and Beyond Disability Solutions Pty Ltd (AABDS) dealings with all participants.

AABDS's Privacy policy and procedure have been framed around participants' rights as they are specified in the Privacy Act 1988, Freedom of Information Act 1982, the Disability Services Act 2006 (QLD) and the National Standards for Disability Services.

Procedures

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

AABDS will:

- Only collect information about the participant that can be shown to be directly relevant to effective service delivery and the organisation's duty of care responsibilities.
- Seek the written consent of the participant, their family, carer or advocate prior to obtaining information from any other source.
- Seek the written consent of the participant, their family, carer or advocate prior to releasing information to any other source.
- Ensure that personal information is stored securely and is not left on view to unauthorised employees or the general public.
- Ensure that only those AABDS employees who need access to the information will be granted access.
- Advise the participant, their family, carer or advocate of the nature of the personal information that is held by the organisation about the participant.
- Advise the participant, their family, carer or advocate of their right to view the information that the organisation keeps in respect to the participant.
- Ensure that personal information about a participant is only held by the organisation as long as it remains relevant to the delivery of effective services and AABDS's duty of care obligations.
- Promptly investigate, remedy and document any grievance regarding privacy, dignity or confidentiality.

Performance standards

The following performance standards must be met to ensure that the procedures specified above are implemented effectively.

- All participants, their family, carer or advocate have been provided with a copy of AABDS's Privacy policy in a format they understand.
- All AABDS employees have been provided with a copy of the organisation's Privacy policy and an employee copy of the policy is kept in each service outlet.
- Participants, their family, carer or advocate have been informed why the information sought is required by AABDS.
- Personal Information consent forms have been completed by the participant, their family, carer or advocate prior to information being collected from other sources.
- AABDS maintains a participant information register that houses all personal information pertaining to a participant.
- Participant files are stored in lockable filing cabinets and files are returned to their proper location as soon as they are no longer required.
- Participant names or other identifying information is not displayed on whiteboards or notice boards that may be viewed by other participants, their family, carer, advocate or the general public.
- Photographic, video or other identifying images are not displayed or aired publicly without the written prior permission of the participant, their family, carer or advocate.
- Participant files have been periodically reviewed to ensure that personal information that is no longer relevant, and unlikely to be relevant in the future, is culled from files.
- Any grievances have been addressed in accordance with the Privacy and Complaints policies.

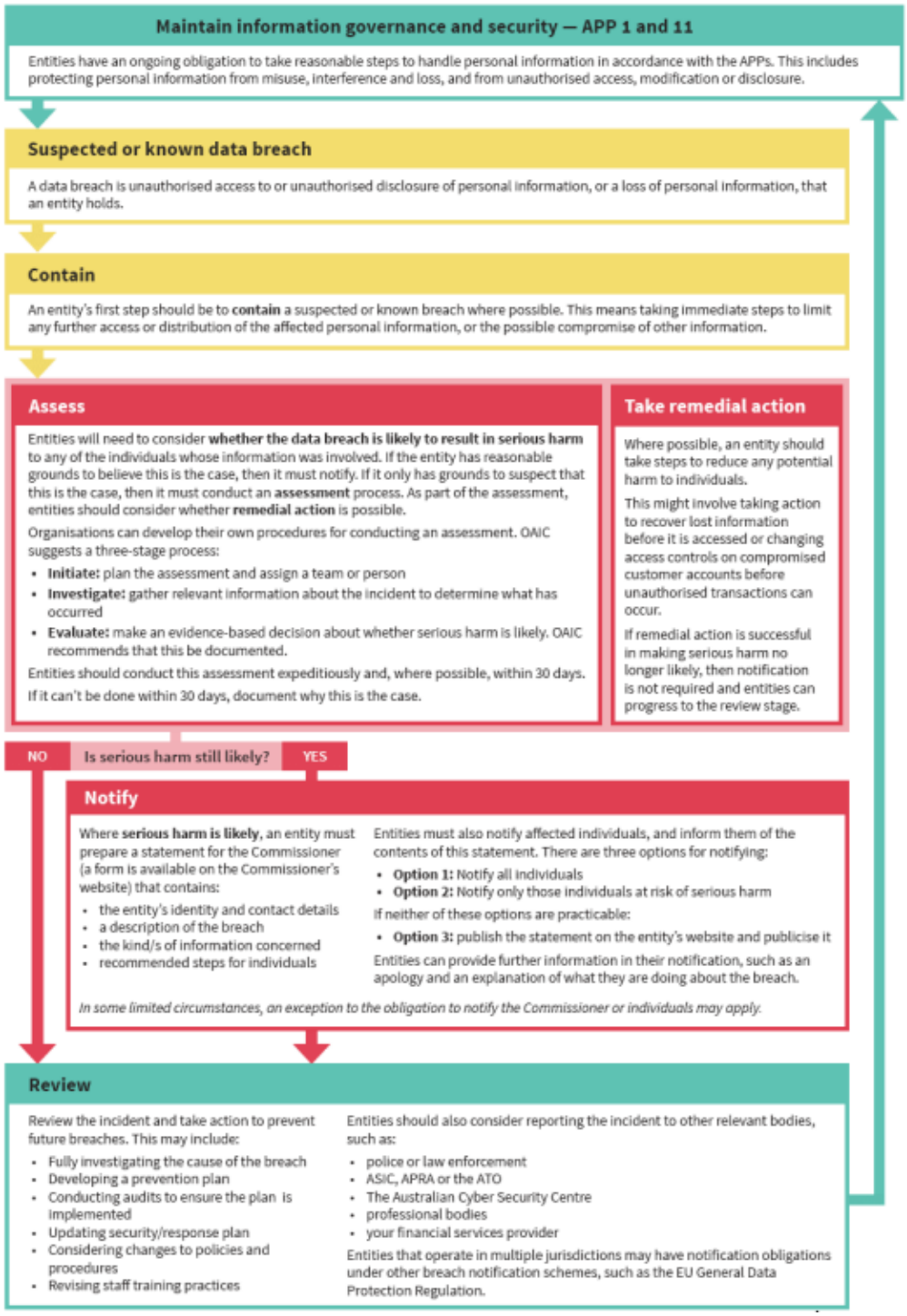
Data Breaches

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

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

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



Identify
AABDS Management will work to determine if a breach has occurred. It is AABDS Management's responsibility to stay informed about the latest scams and ensure staff are trained to recognise a scam to prevent a data breach.

If a breach has happened, AABDS Management will determine the cause and ascertain the seriousness of the breach, including determining:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

During this preliminary stage, AABDS Management will ensure evidence that may be valuable in identifying the cause of the breach or that would enable the entity to address all risks posed to affected individuals or the entitis, is not destroyed.

Contain
AABDS will immediately attempt stop the data leakage, remove the hacker, patch the system and keep evidence of a breach. This involves:

- Determine how to stop the breach from spreading.
- Eliminate the threat.
- Take computers and servers offline.
- Isolate the system.

AABDS Management understands that the quicker the organisation detects and responds to the breach, the less likely it will spiral out of control.

Notify
Under the Notifiable Data Breach (NDB) Scheme and the Privacy Act 1988, AABDS is required to notify any individual at risk of serious harm, including the NDIS Commission, employees, participants, and financial institutions.The organisation may also be required to report the incident to the Office of the Australian Information Commissioner (OAIC).

An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by the organisation (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- AABDS has been unable to prevent the likely risk of serious harm with remedial action.

When reporting a data breach to the OAIC, the organisation must include:

- AABDS's name and contact details;
- a description of the data breach;
- the kinds of information involved;
- recommendations about the steps individuals should take in response to the data breach.

When notifiying AABDS employees, participants and key stakeholders of the breach, AABDS Management will:

- Be open and honest.
- Admit if the issue was the organisation's fault and accept responsibility.
- Provide relevant details.
- Explain why the situation took place.
- Explain the steps that are being taken to resolve the issue.
- Invite dialogue. Discuss the issue with affected parties, key stakeholders, experts, authories, etc., according to the type of breach.
- Educate employee and participants as to how this situation will be prevented in the future.

Change passwords

Once AABSD know the system is 'locked down' and safe, all passwords will be changed by utilising the organisation's IT contractor.

Increase security measures

Once the data breach is resolved, AABDS will revisit and redesign the organisation's security infrastructure to safeguard against future attacks, based on the initial breach.

Responsibility

AABDS employees are responsible for:

- ensuring all participant information is kept and stored in a secure location;
- not disclosing participant information without prior consent;
- having viewed and understood the Privacy policy.

AABDS Managers are responsible for:

- ensuring employees have viewed and understood the Privacy policy;
- ensuring all employees are handling participant information as per the Privacy policy and procedure.

AABDS Directors are responsible for:

- ensuring senior managers are sufficiently skilled and in trained best practice for managing privacy document;
- monitoring the implementation of this procedure.

Reporting

Any grievances or mishandling of participants' private information is recorded in the organisation's complaint register, and as part of the annual reporting process and quality evaluation reports.

Review and evaluation

AABDS will monitor any grievances or mishandling of participants' private information to identify opportunities to improve AABDS's Privacy procedure.

Key contact

Questions about how to implement this procedure should be directed to Kristy McPherson, Director on 0417069124.

PROCEDURE 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
Current version no.	3	Due for review	Feb 2024