# Privacy & Confidentiality Policy

**Policy Statement and Purpose**

Access4u is committed to protecting the privacy of personal and health information which is collected and stored, in line with the *Privacy Act 1988 (Cth)* and will take all reasonable steps to comply with the *Privacy Act 1988 (Cth)* and the thirteen Australian Privacy Principles (APPs) to protect the privacy of any information we may hold.

The purpose of this document is to provide directions when dealing with information that we collect, use and store and applies to all employees, contractors and volunteers.

We will respect the privacy and confidentiality and will ensure that information is managed in appropriate ways.

We collect five broad types of information:

1. Personal information that is recorded information which directly or indirectly identifies a person.
2. Health information about a person's physical or mental health, disabilities or health services received and other information collected in the course of providing services.
3. Sensitive information that is information about a person's race or ethnicity, religious beliefs, sexual preferences or practices, criminal record or membership details, such as membership of a professional association.
4. Business and personal information as part of its normal advocacy and representation, and business operations, including: name, position, organisation, ABN/ACN (where applicable) postal and business address, phone and fax numbers, email address. In some circumstances, for example, where an individual or business is purchasing a product from us paying a fee to us; credit card details or bank details may also be collected.
5. Personal information is collected from donors and supporters for the purpose of processing donations, issuing tax receipts and sending updates.

| **Responsibilities and delegations** | |
|---|---|
| This policy applies to | This policy applies to: all staff and contractors |
| Specific responsibilities | *All staff are required to be aware of this policy and staff working directly with Customers / participants must implement a risk management approach to prevent or minimise the transmission of infection.* |
| Policy approval | CEO |

| **Policy context** – this policy relates to: | |
|---|---|
| Standards | *NDIS Practice Standards* |
| Legislation | *Other than the Privacy Act 1988 (Privacy Act), there are a number of other Australian laws that relate to privacy of personal information including:*<br>*• Collection of Charitable Purposes Act 1939*<br>*• Disability Services Act 1986 (Cth)*<br>*• Personally Controlled Electronic Health Records Act 2012*<br>*• Privacy Amendment (Private Sector) Act 2000 (Cth)*<br>*• Privacy Regulations 2013 (Cth)*<br>*• Privacy Amendment (Notifiable Data Breaches) Act 2017*<br>*• National Health Act 1953* |

| | |
|---|---|
| | • *Health and Community Services Complaints Act 2004 (SA)*<br>• *Healthcare Identifiers Act 2010*<br>• *Telecommunications Act 1997* |
| Contractual obligations | *NDIS Provider Registration* |
| Organisation policies | • Data Breach Response Plan<br>• Information Sharing Policy<br>• Record Management Policy |
| Forms, record keeping, other documents | *Request for access to personal information form* |

**Definitions** For the purpose of this procedure the following definitions apply:-

| | |
|---|---|
| **Compliance** | Refers to ensuring that the requirements of laws, regulations, industry codes and standards are met. |
| **Personal Information (section 6(1)) Commonwealth Privacy Act 1988** | Information or an opinion about an identified individual, or an individual who is reasonably identifiable:<br>(a) whether the information or opinion is true or not; and<br>(b) whether the information or opinion is recorded in a material form or not. |
| **Serious Harm** | 'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. |

## Procedure

**Collection We will:**

- Only collect information that is necessary for the performance and primary function of Access4u.
- Notify stakeholders about why we collect the information and how it is administered.
- Notify stakeholders that this information is accessible to them.

**Use and Disclosure We will:**

- Use and / or only disclose information for the primary purpose for which it was collected or a directly related secondary purpose
- Obtain consent from the affected person for other uses
- Take all reasonable steps to keep any and all information collected strictly confidential Personal information will not be revealed, sold, distributed, rented, licensed, shared or passed on to any third party unless consent (whether express or implied) has been granted by the stakeholder, or organisation, or where we are required to do so by law.
- Make information available to state government, local government and non-government organisation service providers and volunteers where there are issues of safety and wellbeing relating to Customers (refer to the Information Sharing Policy for Promoting safety and wellbeing).

**Data Quality We will:**

- Take reasonable steps to ensure the information collected is accurate, complete, up to date, and relevant to the functions we perform.

**Data Security and Retention We will:**

- Safeguard the information we collect and store against misuse, loss, unauthorized access and modification.
- Only destroy records in accordance with our Records Management Policy.

**Openness We will:**

- Ensure stakeholders are aware of this Policy and its purposes.
- Make this information freely available in relevant publications and on the websites.

**Access, Correction and or Complaint**

***Dealing with request for Access***

- We will ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date.
- Individual requests to access or obtain a copy of personal information must be made in writing and addressed to the Privacy Officer
- There is no charge for an employee or volunteer to access personal information that we hold about them; however there may be a charge of 20 cents per page for every page that is copied. Individuals will be advised of how they may access or obtain a copy of their personal information and the applicable fees within ten (10) days of receiving their written request.

**Exceptions to access**

There are situations where we reasonably believe that access to information should not be granted, this is when:

- Access poses a serious threat to life, health or safety of any stakeholder, or to public health or public safety, or
- Access would unreasonably impact on the privacy of other individuals, or
- The request for access is frivolous or vexatious, or
- The information relates to existing or anticipated legal proceedings between Acceess4u and an individual, or
- The giving of access would be unlawful.

**Correction**

- Where a record is found to be inaccurate, a correction will be made. If there is a request to amend a record, but the record is found to be accurate the details of the request for amendment will be noted on the record.

**Complaint**

- A complaint can be submitted to the Privacy Officer where a stakeholder believes there has been a breach of this Policy. The complaint will be investigated and responded to within thirty (30) days of receiving the written complaint.
- Individuals not satisfied with the outcome of their complaint have an option to refer the matter to the Privacy Commissioner, Commonwealth Officer of the Privacy Commissioner, telephone: 1300 363 992 www.privacy.gov.au.

**Anonymity We will:**

• Give stakeholders the option of anonymity when completing evaluation forms or opinion surveys.

**Notifiable Data Breaches**

The Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Privacy Act) establishes requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

**Data breaches requiring notification?**

Any data breach, that is likely to result in serious harm to any of the individuals to whom the information relates will trigger notification obligations to the individual and the Office of the Australian Information Commissioner (OAIC).

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.

Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

Refer to the procedure in the Data Breach Response Plan when there is a concern that a data breach has occurred or is suspected.

When it is considered that reasonable grounds exist to believe that a data breach has occurred, we are obligated to promptly notify individuals at likely risk of serious harm.

The Commissioner must also be notified as soon as practicable and notifications must include the following
information:

- the identity and contact details of the organisation
- a description of the data breach
- the kinds of information concerned and;
- recommendations about the steps individuals should take in response to the data breach.