Confidentiality policy

Purpose and Scope
Access4u is committed to transparency in its operations and to ensuring it is open to public scrutiny. It must also balance this with upholding the rights of individuals to privacy and of the organisation to confidentiality on sensitive corporate matters. Access4u will prevent unauthorised persons gaining access to an individual's confidential records and permit individuals access to their own records when this is reasonable and appropriate. Accordingly, access to some Access4u documents and records will be limited to specified individuals and not be available to others for viewing. This policy applies to the internal records, client records and unpublished materials of Access4u.

Responsibilities and delegations	
This policy applies to	Governing Body. Staff and Volunteers
Specific responsibilities	**The Board –** Responsible for ensuring effective governance mechanisms are in place. **The CEO and Managers –** Responsible for monitoring and ensuring adherence to Policy and related procedures. Ensure due diligence and take reasonable steps to ensure Access4u are meeting their obligations. Ensure objectives of the policy are achieved. **Staff –** Responsible for adherence to this and related policies, procedures and forms that support this policy.
Policy approval	CEO

Policy context – this policy relates to:	
Standards	National Disability Insurance Scheme Quality and Safeguarding Framework
Legislation	• National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018 • Other than the Privacy Act 1988 (Privacy Act), there are a number of other Australian laws that relate to privacy of personal information including: o Collection of Charitable Purposes Act 1939 o Disability Services Act 1986 (Cth) o Personally Controlled Electronic Health Records Act 2012 o Privacy Amendment (Private Sector) Act 2000 (Cth) o Privacy Regulations 2013 (Cth) o Privacy Amendment (Notifiable Data Breaches) Act 2017 o National Health Act 1953
Contractual obligations	NDIS Code of Conduct

© Access4U 2025. Uncontrolled when printed. Current version can be obtained from Access4u O drive

Organisation policies and procedures	Data Breach Response Plan Information Sharing Policy Filing and Record Management Policy Client record policy Privacy policy
Forms, record keeping, other documents	Request for access to personal information form Access4u Welcome Pack A4u Privacy and Personal Information Easy to Read brochure

Procedure

Customer records

Customer records will be confidential to customers, Access4u management, administration and to a customer's relevant Access4u coordinator, practitioner and/or support worker/s.

Information about customers may only be made available to other parties with the consent of the customer, or in the case of state government, local government and non-government organisation service providers where there are issues of safety and wellbeing relating to the Customer (refer to the Information Sharing Policy).

All customer records will be kept securely and updated, archived and destroyed according to Access4u's customer records policy.

Personnel files

A personnel file is held for each staff member and contains:

- contact details and contact details in case of an emergency
- a copy of the employee's contract
- all correspondence relating to job description changes, salary changes, leave entitlements such as long service leave, continuous service leave, unpaid and parental leave.

Access to personnel information is restricted to:

- the CEO, the Senior Manager Specialist Services, the HR advisor
- the individual staff member accessing their own file, on request

In Australia, employee access to personnel files is governed by:

- The Fair Work Act 2009 (Cth)
- The Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs) — mainly APP 6 & APP 12.

While employers are not legally required to provide full access to all personnel records, the Privacy Act does give employees (or contractors) some rights to access personal information held by employers. However, the Act does allow exceptions to this access.

© Access4U 2025. Uncontrolled when printed. Current version can be obtained from Access4u O drive

Corporate records

Corporate records are those that contain confidential or commercially sensitive information about the organisation's business. They include:

- The financial accounts and records
- Taxation records
- Corporate correspondence with the incorporation regulator
- The corporate key and other access or user name information
- Records of staff or other internal meetings
- Project management files
- Contracts between the organisation and other parties

Access to these records is limited to the CEO and nominated Governing body/Management members.

Requests for access – general records

All records and materials not falling into the categories above may be released to the public at the discretion of the CEO.

Any request for access to information should be directed to the Privacy Manager, who will:

- make available to staff or Governing body/Management Committee members information that they are entitled to access
- refer any request from Access4u members or the public for access to the organisation's records or materials to the CEO

In considering a request, the Privacy Manager will take into consideration:

- a general presumption in favour of transparency
- the relevant provisions of the Access4u constitution regarding information to be made available to Access4u members
- the business, legal, and administrative interests of Access4u, including commercial confidentiality and privacy obligations

Where an external party requests access to information that requires staff to devote time to collating, copying or otherwise making material accessible, the CEO may determine a fee to be charged.

Requests for access – customer records

All customers have the right to access their records and advise the organisation about inaccuracies.

Requests for information about customers from outside agencies or individuals will be referred to the CEO. Before any information is released, the Privacy Officer will contact the customer concerned to obtain consent.

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 using a Request for Access to Personal Information Form and addressed to the Privacy Officer
- In some circumstances there may be an administration charge 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

© Access4U 2025. Uncontrolled when printed. Current version can be obtained from Access4u O drive

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.

Appeals

Individuals who are refused access to their own records or information files may appeal by contacting the Senior Manager Specialist Services who will review the decision in the context of this policy.

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

© Access4U 2025. Uncontrolled when printed. Current version can be obtained from Access4u O drive

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.

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.

© Access4U 2025. Uncontrolled when printed. Current version can be obtained from Access4u O drive

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.

© Access4U 2025. Uncontrolled when printed. Current version can be obtained from Access4u O drive