Privacy policy

Purpose and Scope
Access4u is committed to protecting and upholding the right to privacy of all service users, employees and representatives of agencies we deal with. In particular, Access4u is committed to protecting and upholding service users' rights to privacy in the way we collect, store and use information about them, their needs and the services we provide them. Access4u requires all employees to be consistent and careful in the way they manage what is written and said about service users and how they decide who can see or hear this information. Access4u is subject to the Privacy Act 1988 (Cth). The organisation will follow the guidelines of the *Australian Privacy Principles* in its information management practices. Access4u will ensure that: • It meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of service users and organisational personnel; • Service users are provided with information about their rights regarding privacy; • Service users and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature; • All employees understand what is required in meeting these obligations; and • It will adhere to all requirements imposed under the Privacy Act 1988 (Cth), as amended from time to time.

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: ○ Collection of Charitable Purposes Act 1939

	○ Disability Services Act 1986 (Cth) ○ Personally Controlled Electronic Health Records Act 2012 ○ Privacy Amendment (Private Sector) Act 2000 (Cth) ○ Privacy Regulations 2013 (Cth) ○ Privacy Amendment (Notifiable Data Breaches) Act 2017 ○ National Health Act 1953
Contractual obligations	NDIS Code of Conduct
Organisation policies and procedures	Data Breach Response Plan Information Sharing Policy Filing and Record Management Policy Client record policy Confidentiality 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

Definitions for the purpose of this policy the following definitions apply:	
Word	**Definition**
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: (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.
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.

This policy conforms to the Privacy Act 1988 (Cth) and the Australian Privacy Principles which govern the collection, use and storage of personal information.

This policy will apply to all records, whether hard copy or electronic, containing personal information about service users, and to interviews or discussions of a sensitive personal nature.

Procedure

Dealing with personal information

In dealing with personal information, Access4u employees will:

- Ensure privacy for service users, employees or Board members when they are being interviewed or discussing matters of a personal or sensitive nature;
- Only collect and store personal information that is necessary for the functioning of the organisation and its activities;
- Use fair and lawful ways to collect personal information;
- Collect personal information only by consent from a service user;
- Ensure that people know what sort of personal information is held, what purposes it is held it for and how it

is collected, used, disclosed and who will have access to it;
- Ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any service user to review information or correct wrong information about themselves;
- Take reasonable steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure;
- Destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired; and
- Notify service users and the Office of the Australian Information Commissioner (OAIC) when there has been a data breach (or suspected breach) of personal information, if it is likely to result in serious harm to service users whose privacy has been breached.

Access4u will take all reasonable steps to prevent and manage personal information from being misused, and to keep private information secure. This includes both organisational measures such as delegated responsibilities for managing privacy, deactivating accounts when employees leave, ongoing staff training and technical measures such as multifactor authentication, encrypting sensitive data.

Responsibilities for managing privacy

All employees are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.

The CEO is responsible for content in Access4u publications, communications and website and must ensure the following:

- Appropriate consent is obtained for the inclusion of any personal information about any individual including Access4u personnel;
- Information being provided by other agencies or external individuals conforms to privacy principles; and
- 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.

The CEO is responsible for safeguarding personal information relating to Access4u employees and contractors.

Privacy Contact Officer

The Privacy Contact Officer will be the Senior Manager Specialist Services. The Senior Manager Specialist Services will be responsible for:

- Ensuring that all workers are familiar with the Privacy Policy and administrative procedures for handling personal information;
- Ensuring that service users and other relevant persons are provided with information about their rights regarding privacy; and
- Handling any queries or complaint about a privacy issue.

Training and Development

Access4u implements regular employee training to ensure that we are up to date with understanding the technical measures employed to ensure privacy and security. Organisation-wide training will also be enforced to build all employees' ability to detect the evolving threats or breaches of privacy.

Privacy information for service users

At onboarding the Disability Services Manager will inform service users what information is being collected, how their privacy will be protected and their rights in relation to this information.

Unless required by law, consent will be required for any personal data collection including geo-location tracking data and any data shared with an external party. Consent for the collection or use of any personal data must be voluntary, informed, specific, up to date/ current and easily withdrawn. Informed consent means the individual will know how the data is being used and will specify any overseas parties the data may be shared with, whether the organisation will use the data for high-risk activities and how long the organisation will hold and store the data before correctly deactivating the storage.

Managing automated decision-making

Automated decision-making programs are computer systems that make decisions or provide recommendations without direct human intervention. Examples include resume screening, automated patient triage systems, and diagnostic tools that use artificial intelligence, such as for medication management or personalised treatment plans.

Use of automated decision-making programs are recorded and understood when implemented. This includes:

- Computer programs that are substantially or directly related to making a decision that could affect the rights of a service user such as their rights under a contract, agreement or arrangement;
- Computer programs that are substantially or directly related to making a decision that could affect the interests of a service user such as their access to a service or support; and
- Automated programming that uses a service user's personal information.

In such cases Access4u clearly communicates to the service user an outline of:

- The kinds of personal information used in the operation of the computer program;
- The kinds of decisions made solely by the operations of the computer program; and
- The types of decisions directly related to decisions made by the computer program.

Privacy for interviews and personal discussions

To ensure privacy for service users or workers when discussing sensitive or personal matters, Access4u will provide private meeting rooms and office spaces for employees to use when discussing sensitive or personal matters in face-to-face meetings, online meetings or by telephone.