Privacy and Confidentiality Policy

Introduction
Your Way Disability SA (YWDSA) is committed to safeguarding the privacy and confidentiality of all personal and sensitive information collected, used, and stored in the course of service delivery. This policy ensures compliance with relevant privacy laws and outlines how YWDSA protects participant and staff information.

Applicable When and Who This Applies To
This policy applies to:

- **All YWDSA employees, contractors, and volunteers**, who are responsible for upholding privacy and confidentiality standards.
- **Participants and their representatives**, ensuring their personal information is handled appropriately.
- **Regulatory bodies**, ensuring compliance with privacy laws and best practices.

This policy applies when:

- Collecting, storing, using, or disclosing personal or sensitive information.
- Managing participant and staff records.
- Handling requests for access to information.

Governing Regulations and Compliance
This policy aligns with:

- **Privacy Act 1988 (Cth)**
- **Australian Privacy Principles (APPs)**
- **NDIS Practice Standards and Quality Indicators**
- **NDIS Code of Conduct**
- **Health Records Act 2001 (SA)**
- **Freedom of Information Act 1991 (SA)**

Privacy and Confidentiality Guidelines
YWDSA follows strict privacy and confidentiality guidelines to ensure:

- Only necessary information is collected for service delivery and compliance.
- Informed consent is obtained before sharing participant information.
- Strict access controls are in place to protect sensitive data.
- Personal information is used only for its intended purpose.
- Records are securely stored and only accessed by authorised personnel.
- Confidentiality is maintained in all forms of communication.

Our Commitment to Privacy and Confidentiality
YWDSA is committed to:

- Protecting participant and staff personal information.
- Ensuring compliance with privacy regulations.
- Providing training on privacy and confidentiality obligations.
- Responding to privacy breaches swiftly and effectively.

What Information We Collect and How We Use It

YWDSA collects and uses personal information to provide high-quality services, including:

- Participant details (name, contact information, NDIS plan details).
- Health and medical information (with consent, for service provision).
- Financial details (billing and funding purposes).
- Employment records (for staff and contractor management).

All information collected is used solely for service provision, compliance, and operational requirements.

How We Store and Secure Information

- Electronic records are securely stored using encrypted, password-protected systems.
- Paper records are kept in locked filing systems with restricted access.
- Information is retained and destroyed in compliance with legal requirements.
- Access controls ensure only authorised personnel can view sensitive data.

Data Breaches

YWDSA takes all reasonable steps to prevent data breaches. In the event of a data breach:

1. Containment – Identify and secure the breach to prevent further exposure.
2. Assessment – Determine the nature and scope of the breach.
3. Notification – Inform affected individuals and relevant authorities.
4. Prevention – Implement measures to prevent future breaches.

YWDSA follows Notifiable Data Breach (NDB) Scheme requirements under the Privacy Act 1988.

Breach of Privacy and Confidentiality

A breach of this policy occurs when:

- Confidential information is disclosed without consent.
- Records are accessed, altered, or shared inappropriately.
- Privacy obligations are not followed.

Consequences of a Breach:

- Formal investigation and corrective actions.
- Additional training and supervision where necessary.
- Disciplinary measures, including potential termination for serious breaches.
- Reporting to relevant authorities, including the NDIS Commission, if required.

Monitoring and Compliance

- Regular staff training on privacy obligations.
- Annual review of privacy and confidentiality practices.
- Participant feedback mechanisms to ensure trust in data protection.
- Ongoing security assessments to prevent data breaches.