

## Privacy and Confidentiality Policy

Policy Area:	Operations	Document Owner:	CEO
Doc ID:	OP_POL_011	Date Created:	July 2014
Date of Last Review:	April 2020	Version:	1.6
Date of Next Review:		April 2022	

## Policy Context

Relevant service standards: <ul style="list-style-type: none"> <li>• NDIS Practice Standards: Privacy and Dignity</li> <li>• NDIS Practice Standards: Information Management</li> </ul>	Legislation/other requirements: <ul style="list-style-type: none"> <li>• NDIS Act 2013</li> <li>• Disability Act 2006</li> <li>• United Nations Convention on the Rights of Persons with Disabilities</li> <li>• Privacy Act (Cwlth) 1988 as amended in 2000</li> <li>• Australian Privacy Principles 2014</li> <li>• Information Privacy Act 2000</li> <li>• Health Records Act 2001 (Victoria)</li> </ul>
---	---

### Purpose

To ensure that the privacy and confidentiality of all individuals is respected.  
 To meet relevant service standards, regulatory requirements and comply with all relevant legislation.

### Scope

This policy relates to the Board, CEO, all staff, including volunteers, students and independent contractors, and all participants of Distinctive Options.

### Policy Statement

Distinctive Options is committed to recognising and respecting each individual's right to privacy and confidentiality in all aspects of his or her life. Distinctive Options will ensure potential and existing participant confidentiality and privacy is respected and maintained at all times.

### Policy Details

Distinctive Options ensures that it:

- complies with the privacy principles contained within relevant legislation,
- treats individuals with dignity and respect in all aspects of their lives, and
- maintains the confidentiality of all personal information relating to employees and participants it collects, holds and administers. Personal information is information which directly or indirectly identifies an individual.

Distinctive Options has adopted the following principles in relation to the handling of personal information that are consistent with relevant legislative requirements.

Distinctive Options will:

- collect only information which the organisation requires for effective service delivery;
- ensure that participants are informed as to why we collect the information and how we use the information gathered;
- use and disclose personal information only for our primary functions or a directly related purpose, or for another purpose with the individual's consent (or, where appropriate, the written consent of their legal guardian);
- store personal information securely, protecting it from unauthorised access (including password protection);
- ensure all written, spoken and observed information, and information stored electronically, is treated as private and confidential; and
- provide participants with access to their own information and the right to seek its correction.

Distinctive Options will ensure all participant interviews are conducted in spaces which provide privacy by providing an interview room which is secure and separate from the general workplace.

Distinctive Options staff will not disclose any information related to a participant to other parties whether internal or external except:

- where the release of information has been agreed to by the participant,
- where the sharing of such information is for the purposes of maintaining and/or enhancing service quality or achieving individual outcomes, and/or
- where there is sufficient concern about the safety of the participant or those around them and that information is critical to the safety of the participant or other party.

Distinctive Options has measures in place to ensure individuals' rights to privacy and confidentiality meet, if not exceed, legislative requirements. These measures include not disclosing information about an individual without their explicit consent (or the written consent of their legal guardian) except:

- Non-identifying data required by funding bodies and by government departments for planning purposes;
- Where disclosure is required or authorised by law (such as court subpoena or staff testifying under oath);
- Where it is reasonable that the disclosure is necessary for the enforcement of the criminal law or for a law imposing a fine or for the protection of public revenue;
- Where it is reasonable that the disclosure is necessary to prevent or lessen serious threat to the life or health of the individual or another person; and/or
- Where required as part of the Funding and Service Agreement under which the individual receives access to our services.

These measures also include:

- Holding individual information about a participant in their individual file,
- Ensuring participants are aware of how to access their particular file upon request,
- Providing private meeting rooms/areas when required, and
- Adhering to requirements for archiving and disposal of closed files.

Participants may request to view their information at any time. Participants in receipt of Group Supports are asked if they would like to view their information on scheduled Program Review Days. Requests to view or change information must be made directly to the CEO. Information may be redacted to protect the privacy of other participants or staff.

Distinctive Options recognises that in addition to its legal and contractual obligations in the area of privacy, it demonstrates the values of privacy by the manner in which staff interact and communicate with participants. These privacy values are reflected in and supported by our core values and philosophy.

## Ethical Information Collection

To guarantee that information is ethically collected, Distinctive Options will:

- Ensure that Processes to collect information are in line with legislation
- Ensure that Service Participants consent to collect the information is provided
- Ensure that information is kept confidential and stored safely
- Ensure that Information about the collection of information is provided in ways that the person can understand (e.g. plain English, simple language, pictures, etc.)

## Privacy and Data Breaches

The purpose of notifying privacy breaches is to:

- Ensure timely and effective management of privacy incidents
- Follow up with participants in a timely and respectful manner
- Address contributing factors and develop actions to prevent future privacy breaches
- Assist in identifying systemic issues
- Learn from incidents to improve how participant information is handled

## Reporting Breaches Under the Notifiable Data Breaches (NBD) Scheme

The Notifiable Data Breaches (NDB) scheme is a Commonwealth scheme that requires services to report data breaches “that are likely to cause serious harm to individuals” to the Office of the Australian Information Commissioner (OAIC). Serious harm occurs when the breach is more probably than not likely to cause psychological, emotional, physical, and reputational harm to individuals. For more information about the Notifiable Data Breaches (NBD) Scheme and instructions on reporting a breach, staff should refer to the Data Breach Response and Reporting Plan.

## Procedures

The following procedures are related to this policy:

- [IT Procedure](#)
- [Privacy and Information Security](#)
- [Privacy Incident Reporting](#)
- [Service Delivery Administration Procedure](#)
- [Service Delivery Procedure](#)