

## Privacy and Confidentiality Procedure

Procedure Area:	Operations	Document Owner:	CEO
Doc ID:	OP_PR_002	Date Created:	July 2023
Date of Last Review:	July 2023	Version:	1.0
Date of Next Review:		July 2025	

### Purpose

The purpose of this procedure is to describe how Distinctive Options ensures the privacy and confidentiality of all participants and employees is protected at all times.

### Scope

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

### Procedure

To protect the privacy of all individuals, Distinctive Options will:

- collect only information which the organisation requires for effective service delivery
- ensure that individuals 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 a 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
- provide individuals with access to their own information and the right to seek its correction
- conduct sensitive conversations with individuals in spaces which provide privacy by using a 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 collection and/or release of certain information is a legal, registration or contractual requirement
- where the sharing of such information is for the purposes of maintaining and/or enhancing service quality or achieving individual outcomes
- 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
- 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 or employee in their individual file
- ensuring participants and employees are aware of how to access their particular file upon request
- providing private meeting rooms/areas when required
- adhering to requirements for archiving and disposal of closed files

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 employees.

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
- participants and employees consent to collect the information is provided
- information is kept confidential and stored safely
- information about the collection of information is provided in ways that the person can understand (e.g., plain English, simple language, pictures, etc.)

## **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.

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 information is handled

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](#).

## **Relevant Documents**

The following documents are related to this procedure:

[IT Procedure](#)

[Data Breach Response and Reporting Plan](#)