WORK PRACTICE

Title: Privacy and Confidentiality Policy

Policy Statement and Objective

The purpose of the Privacy and Confidentiality Policy is to guide the practices of Australian Inclusion Group (the Organisation), referenced in its entirety, in establishing standards of privacy and confidentiality in the Organisation's dealings with prospective, current, and past Clients and staff of the Organisation.

The Organisation is committed to protecting the privacy of all the individuals it deals with and will ensure that each individual from whom personal and/or health information is collected, stored, or used, has access to this policy. This is in accordance with the Organisation's obligations under the Privacy Act.

Link to National Standard

This policy is linked to Standard 4 of the National Disability Services Standards, as well as Core Module 1 of the NDIS Practice Standards and Quality Indicators

Guiding Principles

The Organisation is committed to protecting the privacy of all the individuals it deals with. It is bound by the Privacy Act 1988 and undertakes to adhere to the National Privacy Principles.

The Organisation collects personal information in order to provide services to its clients or where it is necessary for the purposes of its activities. The Organisation collects and holds personal information including a person's name and contact details.

All staff must respect the confidentiality of information gained during any work, for the Organisation (both paid and voluntary). All information (i.e., health and personal) relating to any person/s will not be divulged, without authorisation, either now or in the future.

All staff clearly understand that this applies to all information relating to participants in the Organisation's programs, as well as other matters relating to staff and the business of the Organisation. The Organisation uses a variety of physical and electronic security measures. Including restricted physical access to its offices and secure databases, to keep personal information secure from misuse, loss, unauthorised use, or disclosure.

The Organisation agrees that each Client has a right to access most of their personal information. The Organisation reserves the right to deny access to some information in accordance with the Privacy Act and other applicable laws, however, undertakes to advise the client of the reason for this denial.

The Organisation will ensure that each individual from whom personal and/or health information is collected, stored, or used, has access to this policy. This is in accordance with the Organisation's obligations under the Privacy Act.

During induction, new employees must sign the 'Acknowledgement of Policies & Confidentiality Form', within the HR system, to confirm their understanding of all organisational policies and training requirements, and to disclose any conflicts of interest. This digital acknowledgment is automatically recorded in the HR System under their profile.

Organisational Commitments

- **Collection -** Only collect information about the Client that can be shown to be directly relevant to effective service delivery, funding body reporting requirements and the Organisation's duty of care responsibilities.
- **Use and Disclosure -** Seek the consent (written or verbal) from the Client prior to releasing identifying information to any other source. Record this consent in the Client's case notes and/or save written consent in the Client's personal folder.

- **Data Quality -** Information is correct, accurate, and up to date according to the information given to the Organisation
- **Data Security -** Ensure that only those Organisation employees, who need access to the above information, are granted access. Ensure that personal information is stored securely and is not left on view to unauthorised staff, or general public
- **Access and Correction -** Advise the client of their right to view the information that the Organisation keeps in respect to the Client. Clients can have their information amended by contacting the relevant staff at the Organisation.
- **Openness -** Ensure that personal information about a client is only held by the Organisation as long as it remains relevant to the delivery of effective services and the Organisations duty of care obligations.
- Promptly investigate, remedy, and document any Client grievance regarding privacy, dignity, or confidentiality
- **Destruction and disposal -** The Organisation aims to limit paper copy information as this can pose a risk to confidentiality. Staff are to scan paper copies into the Client's file as soon as possible. Staff must then dispose of the paper copies either by shredders or secure bins at office locations
- The Organisation will maintain Client records indefinitely unless the information has been deemed no longer relevant.

Performance Standards

The following performance standards must be met to ensure that the procedures specified are implemented effectively:

- All staff are aware of the agency's policy on privacy and confidentiality, and a copy of the policy is available to all staff.
- Staff records, including recruitment, employee files, complaints, and incidents, are to be treated with the utmost confidentiality. Access to these records is restricted to authorised personnel only, such as the CEO, Managers, or designated HR representatives.
- The confidentiality of staff records is in line with the Organisation's privacy and confidentiality policies, and all staff with access to these records are trained and aware of their responsibilities in maintaining confidentiality.
- Confidential staff information is not disclosed without the explicit consent of the individual, except in circumstances where it is legally required or necessary for the performance of organisational duties.
- The Organisation ensures that staff records are stored securely, with electronic records protected by strong passwords, no hard copy (physical records) are to be printed or kept outside of the staff profile, unless specially requested by authorities. These physical records are destroyed in a secure manner when no longer required.
- Clients are informed when information is required by the Organisation.
- Consent will be provided by clients and volunteers prior to information being given to other external sources.
- The Organisation maintains an information system that houses all personal information pertaining to an individual client in a centralised database. *Reference, Information, Technology, Cyber Security and AI Policy.*
- If client records are required in hard copy form, then these records are stored securely in a non-public place in the office, and files are destroyed as soon as they are no longer required.
- Any personal information contained in computer records is protected by a password, and adheres to the *Information, Technology, Cyber Security and AI Policy*.
- Client full names or other identifying information are not displayed on in clear view of other staff, clients, or the general public.
- Photographic, video, or other identifying images are not displayed or aired publicly without the prior written permission of the Client. In accordance with the *Photography of Children and Vulnerable People Policy.*
- Client records are periodically reviewed to ensure that personal information that is no longer relevant, and unlikely to be relevant in the future, is archived.
- Any grievances have been addressed in accordance with the privacy, dignity and confidentiality principles outlined, *Staff Code of Conduct Policy, External Complaints Policy, Internal Employee Complaints Policy, Poor Performance Management Policy and Whistleblower Policy.*

Version History Table:

Version	Version Date	Authorised Officer	Amendment Notes	Next Review Date
1.3	31/03/2020	Exec Committee	AIG policy created	March 2022
13.0	12/08/2024	Exec Committee	Bi-annual review, separated out policy from procedure	Aug 2026
13.1	20/02/2025	Nikki Ilich	Company banner changed	**Aug 2026**
Complete minor and major version history are managed through SharePoint				

References

Code of Conduct Policy
External Complaints Policy
External Complaints Process - Flow Diagram
Whistleblower Policy.
Internal Employee Complaints Policy
Poor Performance Management Policy
Information, Technology, Cyber Security and AI Policy
Photography of Children and Vulnerable People Policy.

Version History Table:

Version	Version Date	Authorised Officer	Amendment Notes	Next Review Date
1.3	31/03/2020	Exec Committee	AIG policy created	March 2022
13.0	12/08/2024	Exec Committee	Bi-annual review, separated out policy from procedure	Aug 2026
13.1	20/02/2025	Nikki Ilich	Company banner changed	**Aug 2026**
Complete minor and major version history are managed through SharePoint				