Privacy and Confidentiality Policy

1.0 Purpose

This policy explains how Assist Community Services collects, uses, shares, stores, keeps and destroys personal information, and how we respect the privacy and dignity of the people we support, including in their own homes.
It supports Assist to meet the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), the NDIS Code of Conduct and the NDIS Practice Standards, including the Core Module outcomes for Privacy and Dignity and Information Management, and the SIL Module (from 1 July 2026).

2.0 Scope

This policy applies to all staff, contractors, volunteers and work placement students. It covers personal information about participants, their families and supporters, staff, applicants and anyone else, in any form (paper, electronic, photos, audio and video). Employee records may be exempt from parts of the Privacy Act, but Assist still handles staff information in line with this policy.
This document is also Assist's APP privacy policy. An Easy Read privacy summary is given to participants at intake.

3.0 Policy statement

Every person we support has the right to privacy and dignity, in their home, in their personal care and in how their information is handled. Assist only collects the information it needs, tells people why, asks for their consent, keeps it secure, shares it only when the person agrees or the law allows, and treats a breach of privacy as a serious matter.

4.0 Key terms

- **Personal information**: information or an opinion about an identified or reasonably identifiable person (for example name, address, photo, NDIS number). **Sensitive information** (health, disability, ethnic origin, religion, sexuality, criminal record, biometrics) needs extra care and, in most cases, consent to collect.
- **Data breach**: personal information is lost, or accessed or disclosed without authority (for example a lost phone, a misdirected email or a hacked account).
- **Decision-supporter**: a person the participant chooses to help them decide, such as family or an advocate. A **guardian** or **nominee** has formal legal authority.

5.0 Collecting and using information

5.1 What we collect and why

Assist collects information that is reasonably necessary to deliver and plan supports, keep people safe, meet NDIS and legal obligations, manage our workforce, and improve our services. For participants this may include contact details, NDIS plan and funding details, health, medication and disability information, support and

behaviour support plans, risk assessments, case notes, incident records, and the contact details of family, supporters and other providers.

5.2 How we collect it

We collect information directly from the person where we can, through intake and service agreement meetings, forms, phone calls, emails and day-to-day support. With consent, we may collect it from others, such as their guardian, family, support coordinator, health professionals or the NDIA.

When we collect information, we tell the person (in the language and format they understand best) what we are collecting, why, who we usually share it with, what happens if they do not provide it, and how to access it or make a complaint. This includes photos, audio and video recordings.

5.3 How we use it

Information is only used for the purpose it was collected for, or a directly related purpose the person would reasonably expect, unless they consent or the law requires or allows otherwise. Staff may only look at the records they need for their role. Looking up a participant's or colleague's information out of curiosity is a breach of this policy.

5.4 Accuracy

Staff keep records accurate, complete, objective and up to date, written at the time or as soon as possible after, in line with the Support Provision and Case Notes Policy and Procedure.

6.0 Consent and sharing information

6.1 Consent

At intake, and when their service agreement is reviewed, each participant is asked for their consent to collect, use and share their information, including details of who it may be shared with and why. Consent must be informed, voluntary, current and specific, and the participant can change or withdraw it at any time. Consent is recorded on the participant's file using the consent form.

Participants are supported to make their own decisions about their information, in line with the Informed Decision Making Policy. Where a participant does not have capacity to consent to a particular decision, consent is sought from their legally appointed guardian or attorney for that matter, or from their statutory health attorney for health matters, under the Guardianship and Administration Act 2000 (Qld) and Powers of Attorney Act 1998 (Qld). The participant is still involved as much as possible. Verbal consent may be accepted where needed and must be recorded straight away with the date, who gave it and what it covers.

6.2 Sharing with family, decision-supporters and other providers

Family members and decision-supporters do not automatically have a right to a participant's information. Staff only share what the participant has agreed to share,

with the people they have named. If a participant has a guardian, staff share the information the guardian needs for the decisions they are appointed to make.

6.3 Sharing with housemates in SIL

Participants in a shared home do not have a right to each other's information. Staff must not discuss one resident's health, behaviour, finances, incidents, family matters or plans with another resident or their family. Where something about one resident affects others (for example a change in routine, a health risk, or a behaviour support strategy that affects shared spaces), staff only share the minimum needed, and with the resident's consent where possible. Handovers, phone calls and conversations about a resident are held privately, away from other residents and visitors. House communication books, whiteboards and rosters must not show personal information about residents.

6.4 Sharing without consent

Assist will only share personal information without consent where the Privacy Act allows, for example where:

- it is required or authorised by law, such as reportable incidents, NDIA or NDIS Commission requests, court orders, or child safety reporting;
- it is needed to lessen or prevent a serious threat to someone's life, health or safety, and it is unreasonable or impracticable to get consent;
- it is needed to act on suspected unlawful activity or serious misconduct, or for a law enforcement body.

Only the Privacy Officer, General Manager or Operations Manager may approve sharing without consent, except in an emergency, where staff should do what is needed to keep people safe (for example call 000) and tell their manager straight away. Every such disclosure is recorded on the file (what, to whom, why, approved by). The person is told unless this would put someone at risk or the law prevents it. Information sent to others is sent securely, to a confirmed recipient, and contains only what they need.

7.0 Privacy in the home and in daily support

A SIL house is the participants' home. Staff must:

- **Own room**: treat a participant's bedroom and bathroom as private. Knock and wait for permission before entering, unless there is an immediate safety risk. Do not go through a participant's belongings without their consent.
- **Personal care**: provide personal care in private, with doors closed and only the staff who need to be there.
- **Mail**: give participants their mail unopened. Only open mail if the participant asks for help, or if their guardian or administrator has authority and it relates to their role.
- **Phone, internet and devices**: respect participants' right to make and receive private calls, messages and online contact. Staff must not read participants' messages or use their devices without consent.

- **Visitors**: respect participants' right to have visitors in private, in line with the SIL Living Arrangements Policy and Procedure. Staff do not tell visitors about other residents.
- **Photos, video and social media**: never take or share photos, video or audio of participants on personal devices or personal social media. Photos for Assist purposes (such as newsletters, social media or marketing) need the participant's (or guardian's) specific written consent for each type of use, can be withdrawn at any time, and are only taken on Assist devices.

7.1 CCTV, cameras and monitoring devices

Assist does not routinely install CCTV, cameras or other monitoring devices in participants' homes. Any monitoring device in a participant's home (for example a sensor mat, door alarm, epilepsy or audio monitor, or a camera in a shared area) must:

- only be used for a clear safety purpose, be the least intrusive option, and be agreed with the participant (or their guardian) and their housemates where shared areas are covered;
- never be placed in bedrooms, bathrooms or toilets unless there is an assessed and documented health need and specific consent;
- be recorded in the participant's support plan and risk assessment, with who can view any recordings, how long they are kept and when the need will be reviewed;
- if it restricts a person's freedom of movement or is used to respond to behaviour, be treated as a possible restrictive practice under the Behaviour Support and Restrictive Practices Policy and Procedure.

Recording private conversations or people in private activities without consent may be a criminal offence in Queensland. Where a participant or family installs their own device, staff should raise it with their Team Leader so the privacy of housemates and staff can be considered.

8.0 Storing, keeping and destroying information

8.1 Security

Assist takes reasonable technical and organisational steps to protect personal information from misuse, interference, loss and unauthorised access, change or disclosure. These include:

- role-based access to the client management system and shared drives, so staff only see what they need, with access removed promptly when someone leaves or changes role;
- multi-factor authentication, strong passwords, up-to-date security software and secure devices, as set out in the IT and Communications Policy;
- paper records kept in locked cabinets or rooms, and not left in cars, communal areas or unattended;
- not sending personal information to personal email accounts, personal devices or messaging apps that are not approved by Assist;

- confidentiality agreements for staff, contractors and volunteers, and privacy training at induction.

Assist stores personal information in Australia. Assist does not send personal information overseas. If this changes, Assist will take reasonable steps to make sure the information is protected to the standard of the APPs, and will update this policy.

8.2 How long records are kept

Participant records (including support records, case notes, incident records, complaints, behaviour support and restrictive practice records, medication records and service agreements) are kept for **at least 7 years** after the record was made or after the participant last received supports from Assist, whichever is later. Incident records, including reportable incidents, must be kept for 7 years under NDIS rules. Records may be kept longer where the law requires, a legal claim or investigation is underway, or the record relates to a child.

8.3 Destroying records

When records are no longer needed and the retention period has ended, they are destroyed securely: paper by shredding or locked secure-destruction bins, and electronic records by permanent deletion, in line with the Document Control Policy and Procedure. Records needed for a complaint, investigation or legal matter must not be destroyed.

9.0 Access and correction

Participants, staff and others can ask to see the information Assist holds about them, or ask for it to be corrected. They can ask in any way: verbally, in writing, by email or with help from a supporter or advocate. Assist will:

- check the person's identity (and the authority of anyone asking for them), and respond within 30 days, at no charge;
- correct information that is inaccurate, out of date, incomplete or misleading, or, if we disagree, explain why in writing and attach the person's statement to the record if they ask.

Access may only be refused or limited where the Privacy Act allows, for example where it would pose a serious threat to someone's life, health or safety, or unreasonably affect another person's privacy (such as a housemate's information in the same record). The Privacy Officer must approve any refusal, give written reasons and explain how to complain.

10.0 Data breaches

All staff must report a suspected or actual data breach to their Team Leader and the Privacy Officer **immediately**, even if they are unsure or caused it. The Privacy Officer leads the response with the Operations Manager, following these steps:

- **Step 1, contain**: act straight away to stop or limit the breach, for example recall or ask for deletion of a wrongly sent email, change passwords, remotely wipe a lost device, or retrieve paper records.

- **Step 2, assess**: work out what information was involved, whose it is, and whether the breach is likely to result in serious harm to anyone (for example identity theft, financial loss, physical or psychological harm, or humiliation). Health and disability information is high risk. The assessment must be completed quickly, and within 30 days at most.
- **Step 3, notify**: if the breach is an **eligible data breach** (likely to result in serious harm, and the harm cannot be prevented by action we have taken), notify the Office of the Australian Information Commissioner (OAIC) and the affected people as soon as practicable, using the OAIC's notifiable data breach form. Also consider whether the breach is a reportable incident or must be notified to the NDIS Commission, the participant's guardian, the NDIA, police or the Assist insurer.
- **Step 4, review**: record the breach and response in the incident management system, find out why it happened, fix the cause, and report to the General Manager. Every breach, notifiable or not, is recorded under the Incident Management Policy and Procedure.

11.0 Privacy complaints

Anyone can make a complaint about how Assist has handled their personal information or respected their privacy. Complaints can be made **in any way**: in person, by phone, by email, in writing, anonymously, or with help from a family member, advocate or other supporter. A complaint does not have to be in writing. Privacy complaints are managed under the Complaints and Feedback Policy and are referred to the Privacy Officer.

If the person is not satisfied with the outcome, they can complain to the OAIC, or, about NDIS supports, to the NDIS Quality and Safeguards Commission. Serious invasions of privacy can also be the subject of court action under the statutory tort in the Privacy Act, which applies from 10 June 2025. Complaining will not affect a person's supports or employment.

12.0 Artificial intelligence and automated decisions

AI tools (such as chat assistants and note-writing apps) can put personal information at risk if they store or reuse what is entered. No personal information is entered into any AI tool unless the General Manager has approved it after a privacy check.

Where an approved tool is used:

- only the minimum information is used, and a person, not the tool, makes any decision about a participant's supports, funding, rostering, risk or services, and checks the tool's output for accuracy before it is used or recorded;
- participants are told if AI is used to help with their records or supports, in a way they understand.

Assist does not use computer programs to make, or substantially help make, decisions that could reasonably be expected to significantly affect people's rights or interests. All decisions about a person's supports, funding, rostering and risk are made by a staff member.

13.0 Responsibilities

The General Manager is responsible for the final review and approval of this policy and approving AI tools.
The Quality Manager is the Privacy Officer and is responsible for: advice on privacy; access and correction requests; leading data breach assessment and OAIC notifications; privacy complaints with the Complaints and Feedback process; privacy training content; and reporting privacy matters to the General Manager.
The Operations Manager is responsible for making sure services and SIL homes follow this policy, and supporting breach responses.
People and Culture is responsible for the confidentiality and secure storage of staff records, confidentiality agreements, and privacy training records.
Team Leaders are responsible for obtaining and recording participant consents and making sure house practices protect residents' privacy.
Senior Lifestyle Support Workers are responsible for modelling and checking privacy practice in their SIL house. All staff, contractors, volunteers and students are responsible for following this policy, keeping information confidential during and after their engagement, and reporting suspected breaches immediately.

14.0 Communication

Communication about this policy should be implemented in a way that suits each person with regard to their cultural background and communication needs, e.g. use of an interpreter, Easy Read or other accessible formats.
This policy will be:

- communicated to participants, their families, carers and supporters, staff and key internal and external stakeholders of Assist Community Services;
- communicated to current and future staff through induction, team meetings and professional development;
- accessible to all staff through the Assist Community Services policy library.

15.0 Relevant policies and legislation

- Complaints and Feedback Policy; Child Safety and Wellbeing Policy; Whistleblower Policy and Procedure; Incident Management Policy and Procedure; IT and Communications Policy; Document Control Policy and Procedure; Service Agreements Policy and Procedure; Support Provision and Case Notes Policy and Procedure; SIL Living Arrangements Policy and Procedure; Behaviour Support and Restrictive Practices Policy and Procedure; Informed Decision Making Policy; Risk and Rights Decision Guide; Rights and Responsibilities Policy; Workplace Behaviour Policy; Continuity of Support Policy; Code of Conduct
- Privacy Act 1988 (Cth), including the APPs, the Notifiable Data Breaches scheme and the 2024 amendments (Privacy and Other Legislation Amendment Act 2024)
- National Disability Insurance Scheme Act 2013 (Cth); NDIS (Provider Registration and Practice Standards) Rules 2018; NDIS (Incident Management and Reportable Incidents) Rules 2018; NDIS Code of Conduct

- NDIS Practice Standards and Quality Indicators: Core Module (Privacy and Dignity; Information Management) and SIL Module; NDIS Commission SIL Evidence Guide
- Guardianship and Administration Act 2000 (Qld); Powers of Attorney Act 1998 (Qld); Invasion of Privacy Act 1971 (Qld); Child Safe Organisations Act 2024 (Qld); Child Protection Act 1999 (Qld)

16.0 Policy Review

This policy will be reviewed every 3 years, or sooner if circumstances, NDIS rules, external policy or legislation change.

Record of policy development			
Revision	v2.0	**Next Review Due**	October 2029
Owner	Quality Management	**Last Reviewed**	29/10/2026
Approved by	Aalden Pennington	**Date Approved**	29/10/2026