Privacy and Dignity Policy and Procedure

1.0 Purpose

The purpose of this policy is to ensure that the privacy, dignity, and personal information of participants are protected at all times during service provision.

Summit Community Network is committed to maintaining the confidentiality, autonomy, and human rights of every individual. This includes respecting the personal and sensitive information of participants, communicating clearly about how information is collected, stored and shared, and ensuring informed consent is obtained at all stages.

Our goal is to promote safe, person-centred services where participants are treated with dignity and respect, and where their privacy is actively protected in both written and verbal communications.

2.0 Scope

The policy applies to all staff, contractors, and volunteers of Summit Community Network involved in service delivery.

3.0 Policy

Summit Community Network is committed to upholding participants' rights to privacy, dignity, and safety in every interaction. We recognise that breaches of privacy may result in harm, distress, or a breakdown of trust. We will ensure that all personal information is handled lawfully, fairly, and respectfully.

We ensure compliance with the NDIS Practice Standards and Quality Indicators (2021), the NDIS Code of Conduct (2018), the NDIS (Incident Management and Reportable Incidents) Rules (2018), the Privacy Act (1988), and the Australian Privacy Principles.

Participants have the right to:

- Know what personal information is collected and why it is collected.
- Access and request correction of their personal records.
- Refuse or withdraw consent to share information, unless required by law.
- Receive information in their preferred format, including Easy Read, visuals, or through interpreters.
- Be informed of and consent to the use of images, recordings, or personal documentation.
- Expect that their information will be kept private, secure, and only accessed by authorised personnel.

To uphold these rights:

- Summit Community Network will explain to participants, in a way they understand, how their personal information will be managed.
- Consent will be obtained before collecting, recording, or sharing information, and documented appropriately.
- Where personal information is shared externally (e.g. for referrals or advocacy), participant consent must be recorded in writing.
- Audio or video recordings of participants will not occur without written consent and a clear explanation of how the recordings will be used.
- Staff will receive regular training in privacy obligations, respectful documentation practices, and culturally safe communication.

Summit Community Network will use Easy Read documents and communication aids to support participant understanding. Interpreters will be engaged where possible for participants with communication support needs or who prefer to communicate in languages other than English.

All records—whether written, verbal, digital, or visual—will be maintained securely and handled in line with privacy legislation and internal information management procedures.

4.0 Procedure

4.1 Dealing with personal information

In dealing with personal information, Summit Community Network staff will:

- ensure privacy for the participants, staff, or management when they are being interviewed or discussing matters of a personal or sensitive nature

- collect and store personal information that is only necessary for the functioning of the organisation and its activities
- use fair and lawful ways to collect personal information
- collect personal information only with consent from the individual
- ensure that people know of the type of personal information collected, the purpose of keeping the information, the method used when information is collected, used or disclosed, and who will have access to the information
- ensure that personal information collected or disclosed is accurate, complete, and up-to-date and provide access to the individual to review information or correct wrong information about themselves
- take reasonable steps to protect all personal information from misuse, loss and unauthorised access, modification or disclosure
- destroy or permanently de-identify personal information no longer needed or after legal requirements for retaining documents that have expired
- ensure that participants understand and agree with the type of personal information being collected and the reason/s for the collection
- ensure participants are advised of any recordings in either audio or visual format. Before collecting material, the participant's involvement in any recording format has been agreed to in writing

Participants have the right to request access to their personal information, request corrections if information is inaccurate or incomplete, and withdraw consent for non-legally required sharing.
In the event of a privacy breach or unauthorised disclosure, Summit Community Network will:

- Take immediate steps to contain and assess the breach.
- Notify affected individuals where required.
- Comply with obligations under the Notifiable Data Breaches (NDB) scheme of the Privacy Act 1988.
- Review and improve systems to prevent future breaches.

4.2 Participant records

Participant records will be kept confidential and only handled by staff directly engaged in delivering service to the participant. Information about a participant may only be made available to other parties with the consent of the participant, or their advocate, guardian or legal representative. A written agreement providing permission to keep a recording must be stored in the participant's file.

All electronic records will be stored securely in password-protected systems compliant with Australian data protection standards. Staff must not store participant information on personal devices. Any sharing of participant records via email must be encrypted and sent only via secure platforms. All hard copy files of participant records will be kept securely in a locked filing cabinet in the office of the Managing Director.

4.3 Responsibilities for managing privacy

All staff members are responsible for managing personal information to which they have access.
The Managing Director is responsible for:

- managing and responding to privacy breaches in line with the Privacy Act 1988 and NDIS requirements.
- ensuring privacy risks are considered in risk assessments and participant safeguarding plans.
- ensuring that any privacy complaints are investigated fairly and resolved promptly.

The Managing Director is responsible for the content appearing in Summit Community Network publications, communications, and on our website and must ensure:

- appropriate consent is sought and obtained for the inclusion of any personal information about any individual, including Summit Community Network personnel (see Consent Policy and Procedure)
- information provided by other agencies or external individuals conforms to our privacy principles
- our website contains a Privacy Statement that clearly outlines the conditions regarding any collection of personal information from the public captured via their visit to the website

The Managing Director is responsible for safeguarding personal information relating to Summit Community Network's staff, management and contractors. The Managing Director will be responsible for:

- ensuring that all staff members are familiar with the Privacy Policy and administrative procedures for handling personal information
- providing participants and other relevant individuals with information about their rights regarding privacy and dignity
- handling any queries or complaints about privacy issues

4.4 Privacy information for participants

During the first interview, participants are notified of the following:

- the information being collected about them,
- how their privacy will be protected, and
- their rights concerning this data

Information sharing is part of our legislative requirements. Participants must consent to any information sharing between our organisation and government bodies. The participant is informed they can opt out of any NDIS information sharing during audits.

Participants have the right to refuse or withdraw consent for sharing their information with other agencies, unless sharing is required by law or necessary to prevent harm. Staff must clearly explain participants' options and document their decisions.

4.5 Privacy for interviews and personal discussions

When discussing sensitive topics, staff must ensure the environment is private, safe, culturally appropriate, and trauma-informed. Staff should consider the participant's cultural, linguistic, and identity needs and offer interpreter or support person services as required.

To ensure privacy for participants or staff when discussing sensitive or personal matters, Summit Community Network will only collect personal information which is necessary for the provision of support and services and which:

- is given voluntarily
- will be stored securely on the Summit Community Network database.

When in possession, or control, of a record containing personal information, Summit Community Network will ensure that the record shall be protected against loss, unauthorised access, modification or disclosure by such steps as is reasonable in the circumstances. In cases when a record must be provided to a person in connection with the provision of a service to Summit Community Network, everything reasonable will be done to prevent unauthorised use or disclosure of that record.

Summit Community Network will not disclose any personal information to a third party without an individual's consent unless that disclosure is required or authorised by, or under, law.