

Privacy and Dignity

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.

SilaCa Tasmania Pty Ltd 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 SilaCa Tasmania Pty Ltd involved in service delivery.

3.0 Policy

SilaCa Tasmania Pty Ltd 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:

- SilaCa Tasmania Pty Ltd 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.

SilaCa Tasmania Pty Ltd 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, SilaCa Tasmania Pty Ltd 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, SilaCa Tasmania Pty Ltd 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 Manager.

4.3 Responsibilities for managing privacy

All staff members are responsible for managing personal information to which they have access.

The Manager 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 Manager is responsible for the content appearing in SilaCa Tasmania Pty Ltd 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 SilaCa Tasmania Pty Ltd 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 Manager is responsible for safeguarding personal information relating to SilaCa Tasmania Pty Ltd's staff, management and contractors. The Manager 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, SilaCa Tasmania Pty Ltd 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 SilaCa Tasmania Pty Ltd database.

When in possession, or control, of a record containing personal information, SilaCa Tasmania Pty Ltd 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 SilaCa Tasmania Pty Ltd, everything reasonable will be done to prevent unauthorised use or disclosure of that record.

SilaCa Tasmania Pty Ltd 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.

5.0 Related documents

- Code of Conduct Agreement
- Easy Read - Privacy
- Participant Handbook
- Participant Information in Easy English
- Participant Information Consent Form
- Privacy and Confidentiality Agreement
- Staff Handbook
- Staff Training Plan
- Staff Training Record
- Training Attendance Register – In-house
- Consent Policy and Procedure
- Reportable Incident, Accident and Emergency Policy and Procedure
- Advocacy Support Policy and Procedure
- Complaints and Feedback Policy and Procedure
- Management of Data Breach Policy and Procedure

6.0 References

- NDIS Practice Standards and Quality Indicators 2021
- Privacy Act 1988 (Commonwealth)
- Australian Privacy Principles (Commonwealth)
- Notifiable Data Breaches (NDB) scheme — Privacy Act 1988
- National Disability Insurance Scheme Act 2013
- NDIS Code of Conduct Rules 2018
- NDIS (Incident Management and Reportable Incidents) Rules 2018
- NDIS Quality and Safeguarding Framework

Management of Data Breach Policy and Procedure

1.0 Purpose

The purpose of this policy is to ensure that SilaCa Tasmania Pty Ltd maintains a strong commitment to the privacy, dignity, and confidentiality of participants, staff, and stakeholders. This includes the secure management of personal and sensitive information, and a timely and appropriate response in the event of a data breach.

This policy outlines how potential or confirmed data breaches are identified, investigated, recorded, and reported. It ensures that any breach is addressed in a way that mitigates harm, maintains trust, and supports continuous quality improvement across the organisation.

2.0 Scope

The policy applies to all staff involved in managing, handling, or accessing personal and sensitive information.

3.0 Definitions

Term	Definition
Sensitive Information	Subset of personal information and includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation, health information, or criminal record, as defined under the Privacy Act 1988 (Commonwealth).
Participant Data	Any information relating to participants of SilaCa Tasmania Pty Ltd, including but not limited to their NDIS plans, goals, personal circumstances, health records, and other identifying or sensitive information relevant to the delivery of NDIS supports.
Data breach (Eligible data breach)	Unauthorised access to or unauthorised disclosure of personal information or lost personal information in circumstances where unauthorised access to or unauthorised disclosure of the information is likely to occur.
Likely (likely to result in serious harm)	To be interpreted to mean more probable than not

Term	Definition
Reasonable person	A reasonable person is a person who is adequately informed based on information immediately available or following reasonable enquiries or an assessment of the data breach. OAIC's guidance states that: The reasonable person is not to be taken from the perspective of an individual whose personal information was part of the data breach or any other person. Generally, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach.
Likely to result in serious harm	An assessment as to whether an individual is likely to suffer 'serious harm' because of an eligible data breach depends on, among many other relevant matters: • the kind and sensitivity of the information subject to the breach. • whether the information is protected and the likelihood of overcoming that protection. • if a security technology or methodology is used concerning the information to make it unintelligible or meaningless to persons not authorised to obtain it - the information or knowledge required to. circumvent the security technology or methodology • the persons, or the kinds of persons, who have obtained, or could obtain, the information. • the nature of the harm that may result from the data breach.
Potential forms of serious harm	It could include physical, psychological, emotional, economic and financial harm and harm to reputation.
Remedial action	There are several exceptions to the notification obligation. An entity can take effective remedial action to prevent unauthorised access to or disclose information when lost or prevent any serious harm resulting from the data breach. If an entity takes such remedial action, an eligible data breach will not be taken to have occurred. Therefore an entity will not be required to notify affected individuals or the OAIC.

Term	Definition
Suspicion of an eligible data breach	If SilaCa Tasmania Pty Ltd merely suspects that an eligible data breach has occurred, but there are no reasonable grounds to conclude that the relevant circumstances amount to an eligible data breach, we must undertake a “reasonable and expeditious assessment” of whether there are reasonable grounds to believe that an eligible data breach has occurred.
Assessment time frame	Within 30 days after the day, it became aware that the grounds caused it to suspect an eligible data breach.
Personal Information	Personal information includes a broad range of information or opinions that could identify an individual. Personal information will vary depending on whether a person can be identified or identifiable. For example, personal information may include the following: • an individual’s name, signature, address, phone number or date of birth • sensitive information • credit information • staff member record information • photographs • internet protocol (IP) addresses • voiceprint and facial recognition biometrics (because they collect characteristics that make an individual’s voice or face unique) • location information from a mobile device (because it can reveal user activity patterns and habits)

4.0 Policy

SilaCa Tasmania Pty Ltd is committed to maintaining high standards of privacy and confidentiality in line with the NDIS Practice Standards (Rights and Responsibilities, Information Management), the NDIS Code of Conduct, and the Privacy Act 1988, including the Australian Privacy Principles and the Notifiable Data Breaches (NDB) Scheme.

A data breach may occur when personal information held by the organisation is lost or accessed, disclosed, or altered without authorisation. Breaches may result from malicious acts (such as cyberattacks), accidental disclosures, or human error. All data breaches are treated seriously, whether or

not they are eligible for mandatory reporting to the Office of the Australian Information Commissioner (OAIC).

SilaCa Tasmania Pty Ltd will:

- Establish a Data Breach Response Team with appropriate expertise and authority.
- Require all staff to immediately report suspected or confirmed breaches to the Manager.
- Investigate the breach within 48 hours using a Data Breach Process Form.
- Assess the potential harm to affected individuals, particularly those with high vulnerabilities or safeguarding needs.
- Where an eligible data breach is confirmed, prepare and submit a statement to the OAIC using the online Notifiable Data Breach Form, including:
 - Contact details for SilaCa Tasmania Pty Ltd
 - Description of the breach
 - Categories of personal information involved
 - Recommended actions for affected individuals to reduce potential harm
- Notify affected individuals directly by appropriate means (email, phone, letter), or where not practicable, publish the statement on the organisation's website and promote it appropriately.

In all cases, SilaCa Tasmania Pty Ltd will ensure:

- Participants are informed in a culturally sensitive, trauma-informed, and accessible manner.
- The organisation complies with reporting timeframes (no later than 30 days after becoming aware of the breach).
- Data breach records are maintained securely and reviewed for systemic issues.
- Staff receive regular training on privacy, information handling, and breach prevention.
- Trends and learnings from breaches are used to strengthen our information management systems and support continuous improvement.

Where personal data is jointly held by SilaCa Tasmania Pty Ltd and another provider, such as through shared services or subcontracting arrangements, responsibility for notification will be determined in accordance with the data-sharing agreement and only one entity is required to report to the OAIC.

5.0 Procedure

Participants and/or their guardians/advocates affected by any breach must be consulted, informed, and supported in a trauma-informed, culturally appropriate way during the assessment and response.

Safeguarding concerns identified during breach assessments must be escalated in accordance with the NDIS (Incident Management and Reportable Incidents) Rules 2018 and related safeguarding policies.

5.1 Stage 1. Assess and determine the potential impact

- Once notified of the potential data breach, the Manager must consider whether a privacy data breach has (or is likely to have) occurred and made a preliminary judgement as to its possible severity.
- The appropriate managerial staff should seek advice on managing the data breach.
- Criteria for determining whether a privacy data breach has occurred:
 - Is personal information involved?
 - Is the personal information of a sensitive nature?
 - Has there been either unauthorised access to personal information, unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?
- Criteria for determining the severity of the breach:
 - type and extent of personal information involved
 - the number of individuals that have been affected
 - if the information is protected by any security measures (password protection or encryption)
 - type of person/s who now have access
 - whether there is (or could be) a real risk of serious harm to the affected individuals
 - if there could be media or stakeholder attention due to the breach/suspected breach.
- Concerning the above, serious harm could include physical, physiological, emotional, economic/financial or reputation harm, as defined in Section 26WG of the National Data Breach Act.

The Manager and relevant staff will take a preliminary view as to whether the breach (or suspected breach) may constitute a Notifiable Data Breach. Accordingly, the Manager will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team); this will depend on the nature and severity of the breach.

5.2 Stage 2. Select the appropriate data breach management option

If the data breach relates to risks of harm (including abuse, neglect, exploitation), the breach must also be managed in accordance with SilaCa Tasmania Pty Ltd's Reportable Incident, Accident and Emergency Policy and Procedure and Procedure, with prompt escalation to the NDIS Commission as required

Option 1 - Data breach managed at a local level by managerial staff

1. The Manager will ensure the implementation of immediate corrective action if this has not already occurred. Corrective action may include retrieving or recovering personal information, ceasing unauthorised access, and shutting down or isolating the affected system.

2. A Data Breach Process Report must be completed within 48 hours of receiving instructions.
The report will contain a:
 - description of the breach or suspected breach
 - summary of action taken
 - summary of outcomes from the action taken
 - outline of processes implemented to prevent a repeat situation
 - the recommendation that outlines why no further action is necessary
3. The Manager will sign off, confirming that no further action is required.

Option 2 - Data breach managed by the Data Breach Response Team

1. When the Manager instructs that the data breach be escalated to the Response Team, the Manager will convene the Response Team and notify any relevant managerial staff.
2. The Response Team will consist of the following:
 - Director's
 - Human Resource nominee
 - Information Technology nominee
 - Marketing and external relations nominee
 - Other people nominated by the Director's

5.2.1 Primary role of the Data Breach Response Team

There is no single method of responding to a data breach. Each incident must be dealt with case-by-case by assessing the circumstances and associated risks to inform the appropriate course of action. The following steps may be undertaken by the Response Team, as appropriate:

1. Immediately contain the breach if this has not already occurred. Corrective action may include retrieving or recovering personal information, ceasing unauthorised access, and shutting down or isolating the affected system.
2. Evaluate the risks associated with the breach, including collecting and documenting all available evidence regarding the above information.
3. Call upon the expertise of, or consult with, relevant staff members in specific circumstances.
4. Engage independent cybersecurity or a forensic expert, as appropriate.
5. Assess whether serious harm is likely (with reference above and Section 26WG of the National Data Breach Act).
6. Recommend to the Manager whether this breach constitutes an NDB for mandatory reporting to the OAIC and the practicality of notifying affected individuals.
7. Consider developing a communication or media strategy, including the timing, content and method of any announcements to participants, staff members or the media.
8. The Response Team must undertake its assessment within 48 hours of being convened.

5.2.2 Secondary role of the Data Breach Response Team

Once the data breach has been dealt with appropriately, the Response Team should turn its attention to the following steps:

1. Identify lessons learnt and remedial action that can be taken to reduce the likelihood of a recurrence; this may involve a review of policies, processes and refresher training.
2. Prepare a report for submission to senior management.
3. Consider conducting an audit to ensure that the necessary outcomes are affected and effective.

5.3 Stage 3. Notify the Office of the Australian Information Commissioner

- Considering the Response Team's recommendation, the Manager will determine whether there are reasonable grounds to suspect that a Notifiable Data Breach has occurred.
- If there are reasonable grounds, the Manager must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach). In addition to OAIC notification, participants affected by the breach must be provided with clear, accessible, and culturally appropriate communication about the breach, its impacts, and steps taken to protect them. This includes offering additional support or referrals where needed (e.g., advocacy, counselling)

6.0 Related documents

- Staff Training Record
- Staff Training Plan
- Data Breach Process Form
- Reportable Incident, Accident and Emergency Policy and Procedure
- Complaints and Feedback Policy and Procedure
- Advocacy Support Policy and Procedure
- Privacy and Dignity Policy and Procedure
- Consent Policy and Procedure
- Information Management Policy and Procedure

7.0 References

- NDIS Practice Standards and Quality Indicators 2021
- Privacy Act 1988 (Commonwealth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Commonwealth)
- NDIS Code of Conduct Rules 2018
- NDIS (Incident Management and Reportable Incidents) Rules 2018
- NDIS Act 2013 (Commonwealth)
- NDIS Quality and Safeguarding Framework

- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Commonwealth) — keep included
- Australia's Disability Strategy 2021–2031