# Privacy and Confidentiality Policy

*For Soaring Sparrows Pty Ltd*

## 1. Document Control

- **Policy Title:** Privacy and Confidentiality
- **Date Policy Developed:** 10 June 2026
- **Review Date:** 10 June 2027
- **Version:** 2.1
- **Policy Owner:** Director, Soaring Sparrows Pty Ltd

---

## 2. Purpose

This policy explains how Soaring Sparrows Pty Ltd protects the privacy and confidentiality of all participants, staff, and stakeholder information. It ensures that personal and sensitive information is collected, stored, used, and shared in line with legal, ethical, and professional standards.

---

## 3. Scope

This policy applies to all employees, contractors, and representatives of Soaring Sparrows Pty Ltd involved in the collection, storage, use, or sharing of participant information.

---

## 4. What Information is Collected

We collect and store personal and sensitive information relevant to the delivery of services, including but not limited to:

- Personal details (e.g., full name, date of birth, NDIS number, contact details)
- Health and medical information
- Support needs, goals, and plans
- Case notes, reports, and communication records

- Consent forms and service agreements
- Photographs, videos, or images (only with consent – see Section 6)

---

## 5. Why Information is Collected and Shared

Information is collected and shared:

- To identify you
- To deliver safe, effective, person-centred supports
- To meet NDIS compliance and legal record-keeping obligations
- To coordinate services and advocate for participant needs
- To respond to incidents, risks, or emergencies
- To comply with lawful requests (e.g., subpoenas, safeguarding requirements)

---

## 6. How Information is Collected, Stored, and Shared

**Collection:**

- Direct communications with participants and their representatives
- Written documents, forms, and assessments
- Communication with providers or services (with consent)

**Storage:**

- Secure, password-protected cloud-based systems
- Encrypted electronic records with restricted access
- Paper-based records (if used) in locked storage or secure transit cases

**Sharing:**

- Verbally, in writing, or electronically (email, phone, shared systems)
- Only with consent or as required by law or duty of care
- Only with authorised individuals or agencies

---

## 7. Use of Images and Media

### 1. Images for Advertising or Marketing

- Participant images or videos will never be used in advertising, promotional, or social media materials without informed, written consent.
- Consent must specify how and where the image will be used.
- Participants may withdraw consent at any time without it affecting their supports.

2. **Images for Service Delivery (e.g., Assistive Technology or Assessments)**
    - Photos or videos may be used to support assessments or funding applications.
    - These will only be taken and shared with written consent from the participant (or their decision-maker).
    - Images are only shared with the relevant provider and not used for any other purpose.
3. **Images Not Containing Participants**
    - Images that do not include participants (e.g., wheelchair repairs, home modifications, broken equipment) may be shared with providers without participant consent.
    - These images are still treated as confidential and only used for service delivery.

All media files are stored securely in participant records and never kept on personal devices.

---

**8. Use of Digital Dictation Tools (e.g. Microsoft Teams)**

Soaring Sparrows practitioners may use secure digital tools such as Microsoft Teams dictation to help create accurate case notes after meetings or support sessions.

These tools convert spoken words into written text but **do not record or store any audio**. The text is used only to prepare or finalise case notes relating to supports provided.

Before using dictation during a conversation, practitioners will:

- Explain that the tool listens to both voices to generate written notes.
- Confirm that **no audio is recorded or saved**.
- Ask for the participant's **verbal consent** before using the tool.

Participants have the right to **say no** to the use of dictation at any time. If consent is not given, the practitioner will take manual written notes instead.

All written case notes created through dictation are handled in line with Soaring Sparrows' **Privacy and Record Management procedures**, ensuring confidentiality, accuracy, and secure storage.

See Appendix for more information

---

**9. Use of Artificial Intelligence (AI)**

Soaring Sparrows recognises that Artificial Intelligence (AI) tools can assist with administrative tasks, drafting documents, research, and improving workplace efficiency. The use of AI must always protect participant privacy, confidentiality, and comply with legal, ethical, and organisational requirements.

**Use of Public AI Platforms**

Participant information must never be entered into public AI tools or platforms.

This includes, but is not limited to:

- Names
- Personal details
- NDIS numbers
- Progress notes
- Reports, correspondence, or emails containing participant information
- Medical, health, disability, or behavioural information
- Any information that could reasonably identify a participant, their family member, carer, or representative

Public AI platforms (such as ChatGPT, Gemini, and Copilot) are general-purpose tools and may:

- Store information outside Australia
- Retain prompts depending on platform settings or account type
- Use information for system improvement or model training
- Lack healthcare-specific governance and privacy controls
- Not meet the privacy and confidentiality requirements for sensitive participant information

Because of these risks, staff must not enter identifiable participant information into public AI platforms.

**Approved AI Tools**

Where AI is required for participant-related work, staff must use approved organisational systems only.

Currently, Splose AI is the approved AI platform for participant-related activities.

When using approved AI tools:

- Information must only be accessed and used for legitimate service delivery purposes
- Staff must comply with all privacy, confidentiality, and information management requirements
- Participant information must remain within approved organisational systems

Splose AI has been approved because:

- Data is encrypted
- Australian Privacy Principles are supported
- Participant information is protected within the platform
- OpenAI does not retain or use client data for model training under the platform's secured agreement arrangements

**Accuracy and Professional Responsibility**

All AI-generated content must be reviewed by the staff member before use.

Staff remain responsible for ensuring that information generated by AI is:

- Accurate
- Relevant and person-centred
- Professional and appropriate
- Consistent with organisational policies and NDIS requirements

AI-generated content must not be relied upon without human review and professional judgement.

## 10. Participant Consent

Participants (or their appointed decision-maker) will:

- Be informed about what information is collected and why
- Provide written consent before their information or images are shared externally
- Have the right to withdraw or limit consent at any time (unless sharing is legally required)

Consent is documented through:

- Signed Service Agreements
- Consent to Share Information Forms
- Case notes recording verbal consent (if appropriate)

---

## 11. Limits to Confidentiality

Information may be shared without consent if:

- Required by law (e.g., court order, subpoena)
- Necessary to prevent or respond to a serious threat to life, health, or safety
- Required under child protection or safeguarding laws
- Permitted under South Australia's Information Sharing Guidelines (ISG)

Where appropriate and safe, participants will be informed if information is shared without consent.

---

## 12. Responsibilities

**All Staff**

- Protect participant information and maintain confidentiality
- Seek and document consent before sharing information or images
- Report suspected or actual breaches of privacy immediately
- Use Artificial Intelligence (AI) tools in accordance with this policy and never enter participant information into unapproved AI platforms.

**Team Leaders**

- Ensure staff comply with this policy

- Provide guidance and training on privacy and confidentiality

**Director**

- Ensure compliance with privacy laws and NDIS requirements
- Oversee responses to breaches of privacy or confidentiality

---

## 13. Review

This policy will be reviewed annually or sooner if required by changes to legislation, NDIS requirements, or organisational practice.

---

## 14. Related Legislation

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- NDIS Act 2013
- NDIS Practice Standards (Core Module – Rights & Responsibilities, Governance & Operational Management)
- South Australia Information Sharing Guidelines (ISG)

---

## 15. Other Relevant Documents

- Information Sharing and Storage Policy
- Complaints and Feedback Policy
- Incident Management Policy
- Code of Conduct
- Consent Form

---

## 16. NDIS Practice Standards Covered

This policy supports compliance with the following **NDIS Practice Standards**:

**Core Module – Rights and Responsibilities**

- **1.1:** The organisation supports participants to exercise choice and control.

- **1.2:** Participants are informed of their rights, including privacy and confidentiality.
- **1.3:** Participants are informed about how their personal information is collected, used, and shared.
- **1.5:** Organisations take all reasonable steps to protect participant information.

**Core Module – Governance and Operational Management**

- **2.1:** Information management systems are secure and support accurate record-keeping.
- **2.3:** Policies and procedures reflect legal, ethical, and professional standards, including privacy requirements.
- **2.5:** Staff are trained and supported to follow privacy and confidentiality policies.

**Additional Relevant Standards**

- **Participant Records and Documentation:** Case notes, reports, and digital records are managed to ensure accuracy, confidentiality, and accessibility.
- **Use of Technology in Service Delivery:** Digital tools such as Teams dictation are used in a way that maintains privacy, confidentiality, and participant consent.

---

## 17. Approval

Approved By: Kathryn Soar
Position: Managing Director, Soaring Sparrows Pty Ltd
Date: 10/06/2026

---

# Appendix:
# Use of Digital Dictation Tools (e.g. Microsoft Teams) Procedure

**Purpose**

To ensure practitioners use Microsoft Teams dictation and similar tools responsibly and in line with privacy, confidentiality, and NDIS Practice Standards when creating case notes.

**Scope**

This procedure applies to all Soaring Sparrows staff and contractors who use Microsoft Teams or similar tools to assist with case note creation or documentation.

**Responsibilities**

- **Practitioners** are responsible for obtaining verbal consent before using Teams dictation and for ensuring no audio recordings are stored.
- **Supervisors** are responsible for monitoring compliance with this procedure and providing training as needed.
- **The Director** ensures policies and systems support secure information handling and participant privacy.

**Procedure**

**1. Before Using Dictation**

1. Explain to the participant that you would like to use Microsoft Teams dictation to help write accurate case notes.
2. Clarify that Teams dictation:
    - Processes spoken words into written notes.
    - Does **not** record or store any audio or video.
3. Ask for verbal consent by saying:

“Is it okay if I use Microsoft Teams dictation to help me write notes? It listens to what we say but does not record or save any audio.”

4. If the participant agrees, proceed.
5. If the participant declines, take written notes manually.

**2. During the Conversation**

- Use Teams dictation responsibly and only for relevant case note content.
- Avoid discussing unrelated personal information while dictation is active.
- Stop dictation if the participant withdraws consent.

**3. After the Session**

- Review and edit the generated notes to ensure accuracy and professionalism.
- Store the final case note securely in the participant's record management system.
- Delete any temporary text files created during dictation (if applicable).
- Do **not** save or share dictation outputs outside approved systems.

**4. Recording Consent in Case Notes**

Document the consent in your case note, for example:

"Participant gave verbal consent to use Microsoft Teams dictation (no audio recording) to support accurate note-taking."

If consent was not given:

"Participant declined Teams dictation; notes completed manually."

**5. Confidentiality and Data Security**

- Treat all dictated notes as confidential information.
- Follow Soaring Sparrows' Privacy and Record Management Procedures.
- Report any privacy breaches or technical concerns to the Director immediately.

# Appendix: Use of Artificial Intelligence (AI) Procedure

**Purpose**

To ensure Artificial Intelligence (AI) tools are used responsibly, ethically, and in a manner that protects participant privacy, confidentiality, and compliance with legal and NDIS requirements.

**Scope**

This procedure applies to all employees, contractors, students, and representatives of Soaring Sparrows Pty Ltd who use AI tools in the course of their work.

**Responsibilities**

**Staff and Contractors**

- Follow this procedure when using AI tools.
- Protect participant privacy and confidentiality at all times.
- Ensure participant information is only used within approved systems.
- Review and verify all AI-generated content before use.

**Team Leaders**

- Support staff to understand and comply with this procedure.
- Monitor the appropriate use of AI tools within their teams.

**Director**

- Approve AI systems for workplace use.
- Ensure AI tools meet organisational privacy, security, and compliance requirements.
- Investigate any reported breaches involving AI use.

---

**Procedure**

**1. Permitted Uses of AI**

Staff may use approved AI tools to assist with:

- Drafting business policies, procedures, letters, and templates
- Research and information gathering
- Creating training materials
- Administrative tasks
- Proofreading and editing documents
- Developing general resources and communications

All information entered into public AI platforms must be de-identified and must not contain participant information.

---

**2. Prohibited Uses of Public AI Platforms**

Staff must not enter, upload, dictate, paste, or share participant information into public AI tools or platforms.

This includes:

- Participant names
- NDIS numbers
- Dates of birth
- Contact details
- Addresses
- Progress notes
- Reports
- Support plans
- Medical information
- Behaviour support information
- Emails or correspondence containing participant information
- Any information that could reasonably identify a participant, family member, carer, or representative

Examples of public AI platforms include:

- ChatGPT

- Gemini
- Copilot
- Claude
- Perplexity
- Any other publicly available AI system not approved by Soaring Sparrows

---

**3. Approved AI Systems**

Where AI assistance is required for participant-related work, staff must use approved organisational systems only.

Currently, Splose AI is the approved AI platform for participant-related activities.

When using Splose AI, staff must:

- Access information only as required for their role
- Follow organisational privacy requirements
- Ensure outputs are stored within approved systems
- Use professional judgement when reviewing AI-generated content

---

**4. Reviewing AI Outputs**

AI can make mistakes, provide incomplete information, or generate inaccurate content.

Before using any AI-generated material, staff must:

1. Review the content for accuracy.
2. Confirm information is current and relevant.
3. Ensure the content is professional and appropriate.
4. Check that recommendations align with NDIS requirements and organisational policies.
5. Make any necessary corrections before use.

Staff remain fully responsible for all content they create or distribute, regardless of whether AI was used.

---

**5. Privacy and Security Requirements**

When using any AI tool, staff must:

- Protect confidential information.
- Follow the Privacy and Confidentiality Policy.
- Follow the Information Sharing and Storage Policy.
- Use secure passwords and approved systems.
- Report any suspected privacy or security breaches immediately.

---

**6. Reporting Concerns**

Staff must immediately notify their Team Leader or the Director if:

- Participant information has been accidentally entered into an unapproved AI platform.
- An AI tool appears to have disclosed confidential information.
- There are concerns about privacy, security, or data handling.
- AI-generated information may have contributed to an error in service delivery.

Any incident involving AI and participant information will be managed in accordance with the organisation's Incident Management and Privacy Breach processes.

---

**Examples**

**Acceptable Use**

✅ Asking AI to improve a generic letter template.

✅ Using AI to draft a policy.

✅ Using AI to proofread a de-identified report.

✅ Using Splose AI for participant-related documentation where approved.

**Unacceptable Use**

❌ Copying participant case notes into ChatGPT.

❌ Uploading a participant report into Gemini.

❌ Asking a public AI platform to write an email using participant names and personal details.

❌ Entering medical, behavioural, or NDIS information into an unapproved AI system.