



Information Sharing and Storage Policy

For Soaring Sparrows Pty Ltd

Document Control

- **Policy Title:** Information Sharing and Storage Policy
 - **Date Policy Developed:** 15 September 2025
 - **Review Date:** 15 September 2026
 - **Version:** 1.0
 - **Policy Owner:** Director / Privacy Officer, Soaring Sparrows Pty Ltd
-

Purpose

This policy outlines how Soaring Sparrows Pty Ltd securely collects, manages, stores, shares, and protects participant and business-related information. It ensures compliance with legal, ethical, and professional standards, safeguards privacy, and supports safe and effective service delivery.

Scope

This policy applies to all employees, contractors, and representatives of Soaring Sparrows Pty Ltd who collect, handle, store, or share participant or organisational information.

Definitions

- **Personal Information:** Any information or opinion about an identified or identifiable individual, including name, date of birth, contact details, health information, NDIS number, or other sensitive data.
- **Sensitive Information:** Information about a person's health, disability, cultural background, religion, sexual orientation, or other private matters that require special handling.
- **Redacted Material:** Documents or records where personal or sensitive information has been obscured or removed before sharing to protect privacy.

- **Access Request:** A formal request by a participant (or their decision-maker) to view the personal information held about them.
- **Correction/Update:** Changing or updating information to ensure it is accurate, complete, and up to date.
- **Privacy Breach:** Any unauthorised access, use, disclosure, modification, or loss of personal or sensitive information.
- **Participant/Decision-Maker:** The individual receiving services or the person authorised to make decisions on their behalf.
- **Information Sharing:** The process of providing personal or organisational information to authorised individuals or agencies for lawful, necessary, and person-centred purposes.
- **Confidentiality:** The obligation to protect information from unauthorised access, disclosure, or use, and to only share information in accordance with this policy and legal requirements.

Policy Statement

Soaring Sparrows Pty Ltd is committed to:

- Protecting participant and organisational information from loss, misuse, unauthorised access, modification, or disclosure.
- Using secure systems and practices for both digital and physical records.
- Collecting and sharing information only for lawful, necessary, and person-centred purposes.
- Ensuring participants are informed and in control of their personal information, except where legal obligations override consent.
- Taking all reasonable steps to ensure participant information is accurate, complete, and up to date. This includes maintaining and updating personal information when participants advise us of changes and at other times as necessary.
- Retaining and securely disposing of records in line with NDIS and legislative requirements (minimum 7 years).
- Ensuring participants are aware of their right to complain if they believe their privacy has been breached.

This policy should be read together with the Privacy and Confidentiality Policy.

Responsibilities

Director / Privacy Officer

- Oversee secure information management practices.
- Ensure systems and technology meet security standards.
- Manage and respond to information access requests.
- Provide staff training on privacy, confidentiality, and data protection.
- Lead the response to any data breaches.

Staff and Contractors

- Use only company-issued secure systems and devices.
- Collect, store, and share participant information in accordance with this policy.
- Obtain and record informed consent before sharing information externally unless the information meets the conditions for non-consensual sharing.
- Report suspected or actual breaches immediately.
- Follow secure offboarding procedures when leaving the organisation.

Participants / Decision-Makers

- Provide informed consent for information sharing where appropriate.
- Request access to or correction of their personal information.
- Withdraw consent for information sharing at any time (unless disclosure is legally required).

Procedures

1. Information Collected and Stored

- Personal details (name, DOB, NDIS number, contact details, emergency contacts).
- NDIS plans and service agreements.
- Health and medical information.
- Support needs, goals, and risk assessments.
- Behaviour support plans (if applicable).

- Case notes, reports, and communications.
- Consent forms and related records.

2. When Information is Collected

- During intake and onboarding.
- Throughout service delivery (case notes, reports, reviews).
- Following incidents or significant events.
- When liaising with other providers, supports, or family members.

3. Why Information is Collected and Shared

- **To identify you**
- To provide safe, effective, person-centred services.
- To meet NDIS compliance and record-keeping obligations.
- To assist you with your enquiries
- To advocate for participants and coordinate supports.
- To respond to risks, incidents, or safeguarding requirements.
- To comply with lawful requests (e.g. court orders, child protection).
- To comply with legal obligations of staff

4. Digital Storage and Security

- **Splose Client Management System:** Encrypted, role-based access, and two-factor authentication.
- **One Drive:** Password protected and two-factor authentication

Naming Convention – Type of Document, Year Month Day (if necessary),
SURNAME First Name or Initial

Example: Novita OT FCA 2024 Sep DOE J

Novita OT FCA 2024-09-03 DOE John

- **Company-Issued Devices:** Password-protected, encrypted, antivirus/firewall protected, and auto-lock enabled.
- **Personal Devices:** Not permitted unless authorised and encrypted.
- **Password Management:** Complex, unique, regularly updated passwords required. Passwords must not be shared or stored insecurely.

5. Physical Records

- Stored securely in locked cabinets accessible only by authorised staff.
- Hard copies digitised as soon as practicable.
- Secure disposal (shredding) of records when no longer required.

6. Information Sharing

- Information may be shared verbally, in writing, or electronically.
- Sharing occurs only:
 - With informed participant consent.
 - When required by law (e.g. subpoenas, child protection).
 - To prevent serious threats to health, safety, or welfare.
- Information will only be shared with relevant and authorised individuals or agencies.

7. Participant Consent

- Participants (or decision-makers) are informed about what is collected and why.
- Consent is documented in service agreements, consent forms, or case notes.
- Consent may be withdrawn at any time unless disclosure is legally required.

8. Limits to Consent

Information may be shared without consent if:

- Required by law (e.g. Reportable incidents to the NDIS Commission, mandated reports, SA Information Sharing Guidelines, subpoenas, child protection laws).
- Necessary to protect life, health, or safety.

Participants will be informed where safe and appropriate.

Any non-consensual sharing is documented and discussed with the Director or Line Manager.

9. Participant Access to Records

- Participants may request access to the information we hold about them.
- Requests for access must be made in writing and verified.
- Access will be provided within 10 business days unless refusal is legally justified.

- Participants may request corrections if information is inaccurate, incomplete, or out of date
- Corrections, copies, and redactions will be provided as appropriate.
- Participants may make a complaint if they believe their privacy has been breached.
- Accessible formats (Easy Read, interpreters, advocates) will be offered if required.

10. Staff Exits and Offboarding

When a staff member leaves the organisation,

- Access to systems (Spouse, email, devices) are revoked immediately.
- Devices, records, and materials are returned before final day.
- IT systems are audited for unauthorised activity.
- Staff are reminded of ongoing confidentiality obligations.

11. Confidentiality and Training

- All staff sign confidentiality agreements.
- Training is regularly provided on privacy, confidentiality, and ethical handling.
- Breaches of confidentiality may result in disciplinary action.

Records Disposal

Soaring Sparrows Pty Ltd ensures that all participant, staff, and organisational records are securely retained and disposed of in line with legal, regulatory, and contractual requirements.

- **Retention:**
 - Participant records are retained for at least **7 years** after service delivery ends, or until a minor participant turns 25.
 - Staff employment records are retained for **7 years** after employment ends.
 - Financial and business records are retained for **7 years**.
- **Disposal:**
 - Records are securely destroyed once retention periods expire and they are no longer required.

- **Digital records** are permanently deleted, including backups where possible.
 - **Physical records** are shredded or destroyed by an approved secure disposal provider.
 - **Accountability:**
 - All disposals are documented in the **Records Disposal Register**.
 - Disposal must be authorised by the Privacy Officer or Director.
 - Completed Disposal Registers securely retained for auditing.
-

Related Legislation

- **NDIS Act 2013 (Cth)**
 - **NDIS Practice Standards (Quality Indicators) 2018 (Cth)**
 - **Privacy Act 1988 (Cth)**
 - **Work Health and Safety Act 2012 (SA)**
 - **Children and Young People (Safety) Act 2017 (SA)**
 - **Information Sharing Guidelines (SA)**
-

Other Relevant Documents

- Soaring Sparrows Privacy and Confidentiality Policy
 - Soaring Sparrows Participant Rights and Responsibilities Policy
 - Soaring Sparrows Complaints and Feedback Policy
 - Soaring Sparrows Risk Management Policy
 - NDIS Code of Conduct
-


Review


This policy will be reviewed annually or earlier if:

- There are changes in legislation, technology, or NDIS requirements.
- A privacy or data breach occurs.
- Feedback indicates improvements are required.

Contact – Privacy Officer

Soaring Sparrows Pty Ltd

 Email: kathryns@soaringsparrows.com.au

 Phone: 0431 753 950

 Address: 31 Short Rd, Elizabeth SA 5112

Approval

Approved By: Kathryn Soar

Position: Director, Soaring Sparrows Pty Ltd

Date: 19/09/2025



Appendix A – Data Breach Response Procedure

Soaring Sparrows Pty Ltd

Purpose

This procedure sets out the steps Soaring Sparrows Pty Ltd will take in the event of a data breach to protect participants, meet legal obligations, and minimise risk.

A *data breach* occurs when participant or organisational information is:

- Lost,
- Accessed without authorisation,
- Disclosed without consent, or
- Altered/destroyed unlawfully.

Immediate Response – Contain the Breach

1. Identify and contain the breach immediately.
 - Stop unauthorised access (e.g. disable accounts, recover lost devices, shut down compromised systems).
 - Retrieve information where possible.
2. Notify the Director/Privacy Officer as soon as possible.

Assessment – Evaluate the Risks

The Director/ Privacy Officer will:

1. Assess what information was involved (personal, sensitive, financial, health, etc.).
2. Identify who has been affected (participants, staff, stakeholders).
3. Evaluate the potential harm (identity theft, safety risks, loss of dignity, reputational damage).

4. Decide whether the breach meets the threshold for reporting under the **Notifiable Data Breaches (NDB) scheme**.

Notification – Inform Relevant Parties

If the breach is likely to cause **serious harm**:

1. The Privacy Officer must notify:
 - The **Office of the Australian Information Commissioner (OAIC)** under the NDB scheme.
 - The **affected individuals** (participants, staff, or stakeholders).
 - The **NDIS Quality and Safeguards Commission**, if the breach impacts participants or service delivery.
2. Notifications must include:
 - A description of the breach.
 - What information was involved.
 - Recommended steps individuals should take to protect themselves.
 - What Soaring Sparrows is doing to respond.

Remediation – Reduce Future Risks

The following actions may be taken to reduce future risks:

- Reset passwords, strengthen access controls, and update security measures.
- Provide additional staff training if required.
- Review and update policies, systems, and procedures.

Documentation

- All breaches, regardless of severity, must be documented in the **Data Breach Register**.
- Records must include:
 - Date/time of breach.
 - Description of incident.

- Individuals affected.
- Actions taken.
- Outcome of review.

Responsibilities

- **Privacy Officer / Director:** Lead the response, ensure compliance, report to authorities.
- **Staff and Contractors:** Immediately report suspected or actual breaches, follow instructions to contain and remediate.

Review

This procedure will be reviewed annually or after any significant breach to ensure effectiveness.



Appendix B

Control of Records Procedure

Soaring Sparrows Pty Ltd

Purpose

This procedure outlines how Soaring Sparrows Pty Ltd creates, maintains, protects, retains, and disposes of records to ensure compliance with legal, regulatory, and organisational requirements.

Scope

This procedure applies to all participant, staff, and organisational records in both digital and physical formats.

Procedure

1. Creation of Records

- Records must be accurate, complete, and created at the time of the event or activity.
- All participant records must include the participant's full name, NDIS number, and date.
- Digital records must be entered into the **Splose Client Management System** or saved in the **One Drive**.

2. Identification of Records

- Records must be clearly titled and stored under the correct participant or organisational file.
- Each record must be dated and, where relevant, signed or electronically attributed to the author.

3. Access to Records

- Access is restricted to authorised personnel only.
- Role-based access controls are used in Splose to ensure appropriate permissions.
- Hard copy files are kept in locked cabinets accessible only to authorised staff.

4. Storage of Records

- **Digital records:** Stored securely in Splose with encryption, backups, and multi-factor authentication.
- **Physical records:** Stored in locked, fire-resistant cabinets and digitised as soon as practicable.
- **Working notes:** Must be transferred to official records promptly and destroyed if no longer required.

5. Retention of Records

- Participant records must be retained for **7 years** after the end of service delivery, or longer if required by legislation (e.g. for minors, until age 25).
- Employment records must be retained for **7 years** after termination of employment.
- Financial records must be retained for **7 years** to meet taxation obligations.

6. Disposal of Records

- Records that are no longer required must be securely destroyed:
 - **Digital records:** Permanently deleted from systems, including backups where possible.
 - **Physical records:** Shredded or destroyed by an approved secure disposal provider.
- Disposal must be documented in a **Records Disposal Register**, including date, description, and authorisation.

7. Review of Records

- Records will be reviewed regularly to ensure they are up to date, relevant, and compliant.
- The Privacy Officer is responsible for ensuring records are archived or disposed of in accordance with this procedure.

Responsibilities

- **Privacy Officer / Director:** Oversight of record control, compliance monitoring, approval of disposal.
- **Staff and Contractors:** Accurate creation, secure handling, and prompt reporting of record issues.

Documentation

- **Records Disposal Register**
- **Data Breach Register**
- **Staff Training Records**