POLICY: Privacy and Information	**CATEGORY:** Leadership
NDIS PRACTICE STANDARD: 5. Service Access	
AGED CARE STANDARD: 8: Organisational Governance	
DFFH STANDARD: 5. Governance and Management	

1. PURPOSE & SCOPE

SRS to manage and ensure that the rights of the participants remain private and only used for purpose that it is collected. This policy applies to all employees.

2. POLICY

SRS is committed to protecting and upholding the right to privacy of participants, staff, management, and representatives of agencies we work with. We place a strong emphasis on safeguarding the privacy of our participants in the way we collect, store, and use information about them, their needs, and the services we provide.

The Privacy Act 1988 is Australian federal legislation that regulates how personal information is collected, stored, used, and disclosed. It also outlines how individuals can make privacy complaints, the obligations of organisations in the event of an eligible data breach, and how the regulator may investigate privacy breaches. SRS is committed to complying with the Privacy Act and the Australian Privacy Principles in all aspects of our information management.

We require all employees and management to be consistent and careful in how they manage what is written or said about individuals, and in determining who is permitted to access this information. SRS is also subject to oversight by the NDIS Quality and Safeguards Commission, Aged Care Commission, Social Services Regulator, and the Office of the Australian Information Commissioner (OAIC).

SRS will ensure that each participant understands and agrees to what personal information will be collected and why, including any recorded material in audio and/or visual format. We are committed to explaining confidentiality policies in a way that is accessible and appropriate to each participant's preferred language, communication method, and level of understanding.

SRS will ensure that:

- It meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of participants and organisational personnel.

- Participants are provided with information about their rights regarding privacy and confidentiality.
- Participants and organisational personnel are provided with privacy and confidentiality when they are being interviewed or discussing matters of a personal or sensitive nature.
- All staff, management and volunteers understand what is required in meeting these obligations.
- Participants are advised of confidentiality policies using the language, mode of communications and terms that are most likely to be understood. Our company will attempt to locate interpreters and use easy access materials such as those on NDIS website.

This policy conforms to the Privacy Act (1988) and the Australian Privacy Principles which govern the collection, use and storage of personal information.

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, and to interviews or discussions of a sensitive personal nature.

SRS has appointed a Privacy Officer who will be responsible for organisation privacy concerns. The current contact details of our Privacy Officer are:

Name: Aidan White

Email: awhite@srsinc.com.au

Phone: 03 5022 1741

You are required to comply with any directions and requests from the Privacy Officer and the provisions of this Policy (and any updates made by us from time to time) as part of working with us.

3. PROCEDURE

What is the difference between personal and sensitive information?

Under the Privacy Act, personal information refers to any information or opinion that can identify an individual. Within this category, there's a specific type known as sensitive information. This includes things like health details, racial or ethnic background, religious beliefs, and more. Because of its nature, sensitive information is given a higher level of protection than other kinds of personal information.

Below are examples of personal and sensitive information;

Personal information includes	Sensitive information includes
• name; • postal address; • email address; • phone number; • date of birth; • bank account or credit card details; • geo-location data. • health information about an individual; • genetic information about an individual that is not otherwise health information; • biometric information that is to be used for the purpose of automated biometric verification or biometric identification; • biometric templates.	• information or an opinion about an individual's: • racial or ethnic origin; • political opinions; • membership of a political association; • religious beliefs or affiliations; • philosophical beliefs; • membership of a professional trade association; • membership of a trade union; • sexual orientation or practices; • criminal record;

Every SRS staff member who handles personal information is required to have an understanding of the Australian Privacy Principles as found in annexure one, the objectives of the Privacy Act generally, and our internal information security practices.

Dealing with Personal Information

In dealing with personal information, SRS staff will:

- Ensure privacy for participants, staff, or management when they are being interviewed or discussing matters of a personal or sensitive nature.
- Only collect and store personal information that is necessary for the functioning of the organisation and its activities.
- Use fair and lawful ways to collect personal information.
- Collect personal information only by consent from an individual.
- Ensure that people know what sort of personal information is held, what purposes it is held for and how it is collected, used, disclosed and who will have access to it.
- Ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any individual to review information or correct wrong information about themselves.
- Take reasonable steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure.
- Destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired.
- Ensure that participants understand and agree to what personal information will be collected and why.
- Participants will be informed why any recordings occur - audio and/or visual format. These must be agreed to in writing.

All staff are encouraged to raise privacy questions and issues with the Privacy Officer.

Privacy Information for Participants

Participant records will be confidential to participants and staff directly engaged in delivery of service to the participant. Information about participants may only be made available to other parties with the consent of the participant, or their advocate, guardian or legal representative. All participant records will be kept on a securely protected database that is restricted to staff members directly engaged in delivery of service to the participant.

During the intial interview participants will be told what information is being collected, how their privacy will be protected and their rights in relation to this information.

Responsibilities for Managing Privacy

- All staff are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work.
- CEO is responsible for content in SRS publications, communications and website and must ensure the following:
    - Appropriate consent is obtained for the inclusion of any personal information about any individual including SRS staff
    - Information being provided by other agencies or external individuals conforms to privacy principles
    - That the website contains a Privacy statement that makes clear the conditions of any collection of personal information from the public through their visit to the website.
- Privacy Officer is responsible for;
    - Safeguarding personal information relating to Organisation. Name staff, management, contractors.
    - Ensuring that all staff are familiar with the Privacy Policy and administrative procedures for handling personal information.
    - Ensuring that participants and other relevant individuals are provided with information about their rights regarding privacy.
    - Handling any queries or complaint about a privacy issue.

Privacy for Interviews and Personal Discussions

To ensure privacy for participants or staff when discussing sensitive or personal matters, the organisation will:

- Only collect personal information which is necessary for the provision of information provided on the site;
- Which is given voluntarily; and
- Which will be stored securely on the SRS database

When in possession or control of a record containing personal information, will ensure that:

- The record is SRS protected against loss, unauthorised access, modification or disclose, by such steps as it is reasonable in the circumstances to take;
- If it is necessary for that record to be given to a person in connection with the provision of a service to SRS, everything reasonable will be done to prevent unauthorised use or disclosure of that record.

Access request and correction requests

Staff members play an important role in protecting personal information. If you're ever unsure about what to do, it's always best to check in with the Privacy Officer. Below are some common examples to guide you.

Scenario	What You Should Do	Why This Matters
A participant asks to see their personal file.	Inform your Line Manager who will notify the Privacy Officer.	Requests to access personal information must be managed according to privacy laws.
A participant asks you to correct or update their information.	Let your Team Leader or Line Manager know.	Changes to personal information need to follow proper processes.
A participant requests their information be deleted.	Inform your Line Manager who will notify the Privacy Officer.	Deleting information has legal implications and must be approved.
You're not sure if the information you're looking at is considered "personal information."	Check with your Team Leader or Line Manager and they will be able to confirm this for you.	It's important to confirm what qualifies as personal information before acting.

Staff must not respond to the request or charge any access fees until the Privacy Officer has approved it.

Please refer to *Privacy & Data Management Response Guide* for further information.

Data breach obligations

If any staff member suspects or knows that a data breach has occurred or may have occurred, they must inform the Privacy Officer immediately. As a first step, this is best done in-person or via a phone call so that the Privacy Officer can ask questions and quickly respond. If the Privacy Officer is not available, the staff member should send an email to the Privacy Officer requesting an urgent meeting to discuss a possible data breach and should, to the extent possible, inform their manager in-person or via a phone call of the possible data breach.

The *Privacy & Data Management Response Guide* contains more detail on the response of all employees, at different levels, in the event of a data breach.

Endorsed position on ransom payments

SRS unequivocally prohibits the payment of ransoms in response to cyberattacks, including but not limited to ransomware incidents. Under no circumstances shall SRS authorise or facilitate the

payment of any ransom to cybercriminals. All SRS staff are expressly forbidden from paying any ransoms on behalf of the organisation.

Paying ransoms not only fails to guarantee the recovery of compromised data but also fuels the profitability and proliferation of cybercrime. It incentivises perpetrators to target not only SRS but also others within the industry and beyond. By refusing to pay ransoms, SRS mitigates the risk of perpetuating criminal activity and maintains its integrity and responsibility in confronting cyber threats.

Contracting with Third Parties Who Handle Personal Information

If SRS receives personal information from a third party, the third party is required to notify the individual whose information is being shared. This notification should include details about how the information will be used and any other relevant information. If SRS collects the information directly from the individual, we must ensure that the individual is notified in line with privacy laws, with clear and up-to-date information about the collection process.

In addition, it is essential that SRS ensures any contract with a third party that provides or handles personal information includes necessary privacy protections. These protections should include a guarantee from the third party that they are compliant with privacy laws, that the personal information they provide is accurate and up-to-date, and that they are obligated to notify individuals about our collection, when necessary. The contract should also confirm that the third party has the legal right to share this information with SRS without violating any laws or third-party rights.

When sharing personal information with a third party, must verify that the third party complies with all privacy requirements. This means performing due diligence to ensure that the third party has a robust privacy policy, strong security measures, and a history of securely handling data. The contract with the third party must specify that they will only use the personal information for the agreed purposes, protect the information from unauthorised access, and promptly notify us of any data breaches.

SRS has an obligation under privacy laws to inform individuals that their personal information may be disclosed to third parties. This must be included in the Privacy Collection Notice, which should also explain why the information is being disclosed.

4. RELATED DOCUMENTS

- Code of Conduct Form
- Privacy and Confidentiality Agreement
- Privacy Collection Notice
- Policies and Procedures
- Privacy & Data Management Response Guide
- Australian Privacy Principle and How it Applies to SRS

5. REFERENCES

- NDIS Practice Standards and Quality Indicators 2018
- Social Services Act 2023
- Aged Care Act 1997
- Privacy Act (1988)
- Australian Privacy Principles

Annexure One

Australian Privacy Principle (App)	Title	Summary	How It Applies to SRS
APP 1	Open and transparent management of personal information	Requires organisations to manage personal information openly and transparently	SRS maintains a current privacy policy available on our website and follows transparent information practices
APP 2	Anonymity and pseudonymity	Individuals should have the option to not identify themselves.	SRS allows anonymity for general enquiries but requires identification to provide services.
APP 3	Collection of solicited personal information	Only collect information necessary for services, higher standards for sensitive data.	SRS collects only necessary information directly from participants unless impracticable.
APP 4	Dealing with unsolicited personal information	Assess and handle information received unintentionally	SRS reviews unsolicited information and disposes of it if not required or legally collectible
APP 5	Notification of collection	Must notify individuals when collecting personal information.	SRS informs participants why data is collected, how it's used, and obtains consent—especially for audio/visual recordings.

APP 6	Use or disclosure of personal information	Information can only be used for the original purpose or with consent.	SRS uses data for the intended purpose or with participant consent for other uses. Exceptions apply under legal requirement.
APP 7	Direct marketing	Restrictions apply to using data for marketing purposes.	SRS does not engage in direct marketing without clear consent and adheres to the Spam Act.
APP 8	Cross-border disclosure	Must protect data disclosed overseas.	SRS does not share data with overseas entities without consultation with the Privacy Officer.
APP 9	Use of government identifiers	Limits use of identifiers like Medicare or Centrelink numbers.	SRS does not adopt government-issued identifiers as internal identifiers.
APP 10	Quality of personal information	Must ensure information is accurate and relevant.	SRS keeps data updated and checks accuracy before use or disclosure
APP 11	Security of personal information	Must protect data from misuse and unauthorised access.	SRS uses secure systems and protocols to safeguard personal information. Data is destroyed or de-identified when no longer needed.
APP 12	Access to personal information	Individuals must be given access to their personal information.	SRS responds to access requests in line with privacy obligations unless an exception applies.
APP 13	Correction of personal information	Individuals can request corrections to their information.	SRS updates records when corrections are requested and justified. Refusals must be explained.