Title:	1.2.6 PRIVACY AND CONFIDENTIALITY POLICY		
Effective Date:	17 January 2024	**Revision Due:**	17 January 2026

1) Policy Statement/Purpose:

SNCS is committed to protecting and upholding the right to privacy of clients, staff, volunteers, Board members and representatives of agencies we deal with. In particular SNCS is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

SNCS requires staff, volunteers and Board members to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

SNCS will prevent unauthorised persons from gaining access to an individual's confidential records and permit individuals access to their own records when this is reasonable and appropriate. Accordingly, access to some SNCS documents and records will be limited to specified individuals and not be available to others for viewing.

The organisation will follow the guidelines of the Privacy Act (1988) and the Australian Privacy Principles in its information management practices.

SNCS will ensure that:

- it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and organisational personnel
- clients are provided with information about their rights regarding privacy
- clients and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- all staff, Board members and volunteers understand what is required in meeting these obligations
- it will adhere to all requirements imposed under the Privacy Act 1988, including the requirements imposed by the Privacy Amendment (Notifiable Data Breaches) Act 2017, to strengthen the protection of personal information.

2) Principles:

SNCS Privacy Policy and its attached procedures are based on the following principles:

- We only collect personal information about clients that is required by the funding body or needed to provide our services/projects
- We inform our clients why personal information is collected and to whom or to what organisation it is usually disclosed
- We only collect sensitive information such as health information with client consent unless necessary to prevent harm to life or health
- We collect personal information directly from the client unless the client is a minor, under guardianship or has given consent for someone else to provide the information
- We will ensure that the client information we hold is accurate up to date and complete

- We will protect client records from loss, unauthorised access, misuse, modification and disclosure and will ensure their appropriate disposal
- We will provide clients access to their records and tell them how they can get access
- We will allow clients to correct any wrong, incomplete or misleading personal information we hold
- We will not use client information for any other purpose except with client consent unless necessary to prevent harm to life or health
- We will not disclose client information to any other person or organisation without consent unless necessary to prevent harm to life or health
- We only use client identifying codes if necessary and do not use the same codes as other agencies
- We will take all reasonable steps to de-identify health information before it is disclosed for data collection or research purposes

3) Definitions:

- *Personal information* - is regarded as information or an opinion, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

- *Sensitive information* - is information or an opinion about an individual such as race or ethnic origin, political opinions/associations or religious or philosophical beliefs, criminal record, sexual preferences, professional or trade association membership or health information.

  This includes personal and sensitive information that is maintained electronically, in case notes, on video, audiocassette, photographed, written/printed or verbal information given by or about a client to an SNCS staff member. It also includes professional opinion/s if the individual can be identified from that opinion/information.

4) Scope:

This policy applies to all areas of SNCS and its employees, contractors and volunteers and should be read in conjunction with:

- Client Rights Policy
- Client Records & Access to Confidential Information Policy
- Filing & Record Keeping Policy
- Volunteer Workers Policy
- Code of Conduct Policy
- Cyber Security Policy

This policy applies to internal records, clients records and unpublished materials of SNCS.

5) Procedure:

Dealing with personal information

In dealing with personal information, SNCS will:

- ensure privacy for clients, staff, volunteers or Board members 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 staff and clients know what sort of personal information is held, what purposes it is held for and how it is collected, used, stored, disclosed and who will have access to it
- ensure that staff and clients are aware how they can complain about a possible privacy breach
- give individuals the option to be anonymous or use a pseudonym
- 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
- notify individuals and the Office of the Australian Information Commissioner (OAIC) when there has been a data breach (or suspected breach) of personal information, if it is likely to result in serious harm to individuals whose privacy has been breached

SNCS staff need to be aware of the nature and sensitivity of information that is provided to assist us in the provision of services to our staff and clients.

SNCS requires that all staff respect the information provided within the course of administering our work as being confidential, and not to be discussed or provided to any other person(s) without authorisation by the Program Manager.

Under no circumstances shall any information be provided to the media or external agencies without the prior permission of the General Manager.

Privacy information for clients

Client records will be confidential to clients.

In most instances, confidentiality exists between the SNCS team and the client rather than the client and the individual worker. Workers can share relevant information about clients with other members of SNCS without breaching confidentiality. This does not extend to the sharing of information about individual clients with the Board of Management.

In some circumstances, our duty of care responsibilities may override confidentiality provisions. This can happen when:

- there is an obligation not to conceal an intended or actual crime including child abuse, assault, theft or fraud. In these cases, the relevant authorities will be informed
- disclosure is in a client's interest to avoid harm (e.g. suicide)
- there is a need to warn a third party who may be in danger

Informed consent

SNCS only shares and exchanges client information with the client's informed consent. Informed consent means that the client:

- Understands the need to exchange personal information about them.
- Knows what personal information will be exchanged.
- Knows with whom or what agency the information will be exchanged.
- Agrees to the exchange.

Consent may be verbal or written. If verbal, consent is noted on the relevant client's file. Written consent is recorded on our Consent Form, which is attached to the client's file.

In situations where the worker believes that the client may not have the capacity to give informed consent because of their age, mental state or disability, we will attempt to get substitute consent from the client's guardian or appointed representative.

In situations where the client is unwilling to give consent, the need for privacy will be balanced against SNCS' duty of care responsibilities.

Informed Consent - Children and Young People

In situations where there is a need to exchange information about a child or young person, generally consent will be sought from the child's parent or legal guardian. Where appropriate, the child or young person's views will be taken into consideration when making the consent decision.

Section 248 of the Children and Young Persons (Care and Protection) Act 1998 (the Act) provides for the exchange of information relating to the safety, welfare and wellbeing of a particular child or young person or class of children or young persons.

Section 248 of the Act states that the Director-General may furnish a prescribed body with information relating to the safety, welfare and well-being of a particular child or young person or class of children or young people. This allows Department of Communities and Justice (DCJ) to use discretion in the decision to provide information in response to a request for information from a prescribed body under section 248. DCJ will provide the requested information under section 248 only if it is determined by DCJ that the provision of information relates to the safety, welfare and well-being of a particular child or young person or class of children or young persons.

Exchanging information about children and young people to support wellbeing:

Chapter 16A overrides other laws that prohibit or restrict the disclosure of personal information such as the "Privacy and Personal Information Act 1998" and the "Health Records and Information Privacy Act 2002"

Chapter 16A in the Children & Young Persons (Care and Protection) Act 1998 authorises agencies and Non-Government Organisations to share information that helps deliver services and supports to promote the safety, welfare and wellbeing of a child or young person.

Amendments to Section 29 will allow agencies in certain circumstances to disclose reporter details to a law enforcement agency in connection with an investigation into a serious offence alleged to have been committed against a child or young person.

Access to Personal Information

All clients have the right to access their personal information held by SNCS about themselves and their children. They also have the right to correct any information that is incorrect, incomplete or misleading.

This is outlined in the advice given to all clients, taken from SNCS Client Rights Policy, at the start of their relationship with SNCS.

Clients wanting to see their personal records should follow the process in the Client Records & Access to Confidential Information Policy.

Individual family members are **NOT** entitled to access:

- Information about any risk of significant harm reports made to DCJ about their family; in particular, Section 29 of the *Children and Young Persons (Care and Protection) Act 1998* prohibits the release of the identity of any person who has made a risk of significant harm report, or any information from which a person could deduce the identity of a reporter
- Information provided in confidence (e.g. by another agency)
- Information about other people such as:
    - Information about other family members unless those family members consent to the release of their personal information to the person who has requested access (e.g. a natural father cannot access personal information about the natural mother unless the mother consents) or
    - Any "incidental" information records may contain about someone who is not a member of their family (e.g. information about another child at their child's school)

If a person is seeking information that relates to a child over the age of 10, then the child should be consulted prior to making a decision about the release of information. Workers should explain to the child:

- Who is seeking the information
- What information is being sought

In addition to the child's opinion, the following factors should be taken into account:

- the nature of the information requested
- the circumstances in which the information was obtained
- the degree of invasion into privacy
- the motives for the request for information

Requests for information about clients from outside agencies or individuals will be referred to the General Manager. Before any information is released, a worker will contact the client concerned to obtain consent.

Appeals

Individuals who are refused access to their own records or information files may appeal by contacting the General Manager who will review the decision in the context of this policy.

Privacy for interviews and personal discussions

To ensure privacy for clients or staff when discussing sensitive or personal matters, the organisation will ensure all client intake interviews are conducted in a room that is closed to the public. All office desks have privacy screens to ensure staff can make phone calls without other members of staff over hearing the details of the conversations.

Participants in research projects

People being invited to participate in a research project must be:

- given a choice about participating or not
- given the right to withdraw at any time
- informed about the purpose of the research project, the information to be collected, and how information they provide will be used
- given copies of any subsequent publications

The collection of personal information will be limited to that which is required for the conduct of the project. Individual participants will not be identified.

Organisational participants in research projects will generally be identified in SNCS research, unless the nature of a particular project requires anonymity or an organisation specifically requests it.

Board Members

Board meeting minutes will be open to members of the organisation once accepted by the Board, except where the Board passes a motion to make any specific content confidential.

All papers and materials considered by the Board will be open to members of the organisation following the meeting at which they are considered, except where the Board passes a motion to make any specific paper or material confidential.

The minutes, papers and materials from any Sub-Committee meeting will be open to Board members and staff, with the exception of information relating to any matter the Sub-Committee deems confidential.

SNCS membership records

A list of current SNCS Members will be available on request to SNCS members, Board members and staff. Personal information about members (including address and contact details) is confidential and may only be accessed by the General Manager.

Personnel files

A personnel file is held for each staff member and contains:

- contact details and contact details in case of an emergency
- a copy of the employee's contract
- all correspondence relating to job description changes, salary changes, leave entitlements such as long service leave, continuous service leave, unpaid and parental leave

- payroll information such as bank account details, Tax File Number declaration forms and Superannuation Choice form

The staff member has the right to refuse giving their Tax File Number to SNCS, however they will be informed this has income tax and superannuation impacts.

Where the Tax File Number has been disclosed, SNCS will:

- inform the staff member the name of the law (or laws) that authorises SNCS to collect the TFN, the purpose for why it is collected and that they have the right to refuse
- take reasonable steps to ensure that the manner of collection does not unreasonably intrude on the individual's affairs
- take reasonable steps to ensure that information collected is necessary and relevant to the purpose of employment, taxation law or superannuation law

Access to personnel information is restricted to:

- the individual staff member accessing their own file
- the General Manager
- payroll staff

If there are legal proceedings between the staff member and SNCS then the staff member would need to make legal representation to get access to the requested information. If the staff member is no longer an employee then the request for the information will need to be sent to the General Manager. If the staff member is deceased then their estate's legal representative would need to make the request via the General Manager.

Under the TFN Rule, a TFN recipient must not record, collect, use or disclose TFN information unless this is permitted under taxation, personal assistance or superannuation law.

Corporate records

Corporate records are those that contain confidential or commercially sensitive information about the organisation's business. They include:

- The financial accounts and records
- Taxation records
- Corporate correspondence with ACNC/ASIC
- The corporate key and other access or user name information
- Records of staff or other internal meetings
- Project management files
- Contracts between the organisation and other parties

Access to these records is limited to the General Manager and Treasurer and Secretary.

Requests for access – general records

All records and materials not falling into the categories above may be released to the public at the discretion of the Program Manager.

Any request for access to information should be directed to the General Manager, who will:

- make available to staff or Board members information that they are entitled to access

- refer any request from SNCS members or the public for access to the organisation's records or materials to the relevant staff member

In considering a request, the General Manager will take into consideration:

- a general presumption in favour of transparency
- the relevant provisions of the SNCS constitution regarding information to be made available to SNCS members
- the business, legal, and administrative interests of SNCS, including commercial confidentiality and privacy obligations

Where an external party requests access to information that requires staff to devote time to collating, copying or otherwise making material accessible, the General Manager may determine a fee to be charged.

6) Roles & Responsibilities:

The General Manager is responsible for ensuring appropriate strategies and courses of action are implemented in relation to this policy.

The Program Manager is responsible for ensuring staff are aware of their responsibilities.

All staff, volunteers and Board members are responsible for the management of personal information to which they have access, and in the conduct of research, consultation or advocacy work. They must respect and keep confidential internal matters of the organisation and respect the privacy of others.

Staff, after leaving SNCS, may not retain, use or take advantage of confidential information that has been obtained over the course of their official duties.

Program Manager is responsible for content in SNCS's publications, communications and web site and must ensure the following:

- appropriate consent is obtained for the inclusion of any personal information about any individual including SNCS personnel
- 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

General Manager is responsible for safeguarding personal information relating to SNCS staff, Board members, volunteers, contractors and SNCS members.

The Privacy Contact Officer will be the Program Manager. The Program Manager will be responsible for:

- ensuring that all staff are familiar with the Privacy Policy and administrative procedures for handling personal information
- ensuring that clients and other relevant individuals are provided with information about their rights regarding privacy
- handling any queries or complaint about a privacy issue

7) Support & Advice:

If you have any queries relating to this or any other SNCS Policy or Procedure, please do not hesitate to raise your concerns with the General Manager.

8) Tools & Forms:

Client Consent Form [Attachment A]
Privacy Breach Form [Attachment B]
Privacy Breach Assessment Tool [Attachment C]

9) Relevant Legislation

This policy has been developed to be consistent with relevant applicable Federal and State legislation and the objectives, values and guidelines of the individual funding streams.

Key legislation underpinning this policy includes but is not limited to:

- Privacy Act 1988 (Cth)
- Privacy and Personal Information Protection Act 1998 (NSW)
- Crimes Act 1900 (NSW)
- Children & Young Person's (Care & Protection) Act 1998
- State Records Act 1998 (NSW)
- Electronic Transactions Act 1999 (Cth)
- Anti-Discrimination Act 1991 (Cth)
- Anti-Discrimination Act 1977 (NSW)
- Family Law Act 1975 (Cth)
- Australian Privacy Principles

10) Amendment History:

This policy shall remain current unless further reviewed or amended. This policy shall be reviewed within a 2 year period.

ATTACHMENT A

CLIENT CONSENT FORM

I,……(name), of

…….(address)

agree to relevant information, which includes personal and health information, being exchanged with agencies listed on this consent form and for each of those agencies discussing between themselves information about myself for the purpose of providing support services.

Agency Name	Team or Unit (if relevant)

I understand that:

- If I do not sign this form, I will still be able to get available services directly
- I can change my mind and withdraw my consent in writing
- Information about child protection issues or law and safety matters may be required to be given to all relevant agencies
- SNCS Privacy Policy has been explained to me

Declaration:

The need to exchange my personal information with other agencies has been explained to me.

I agree to my information being exchanged

Signed……

Date……..

This form is valid until……

ATTACHMENT B

PRIVACY BREACH FORM

This template has been designed to assist agencies to manage a privacy breach involving personal information and to capture a record of the steps taken to contain or control the situation and the decisions made.

Report prepared by:	Name: Job Title: Business unit: Date:
1. What type of personal information is involved?	Choose all that apply: ☐ Personal details such as name or date of birth ☐ Contact information such as home address, phone number or email address ☐ Financial information such as credit card number/s ☐ Tax File Number ☐ Identifiers such as licence number, Medicare number or Student identifier ☐ Other – please specify
2. Number of individuals whose personal information is involved in the breach (if known)	☐ 1 ☐ 2 – 10 ☐ 11 – 50 ☐ 51 – 100 ☐ Greater than 100
3. Date of breach	Date: Or provide best estimate if date not known:
4. Date of discovery (provide best estimate if exact date not known)	Date: Or provide best estimate if date not known:
5. Primary source of breach	Choose all that apply: ☐ Human error: ☐PI sent to wrong recipient (email) ☐PI sent to wrong recipient (mail) ☐PI sent to wrong recipient (other) ☐Failure to use BCC when sending email ☐Other (please specify) ☐ Unauthorised disclosure or use ☐ Loss of hardware, documents or data ☐ Insecure disposal ☐ Malicious or criminal attack: ☐Cyber incident (eg Phishing, Ransomware, hacking, malware) ☐Social engineering/impersonation ☐Rogue employee/insider threat ☐ Other – please provide details ☐ Currently unknown

6. How did the breach occur (if known)	
7. Is there a risk of serious harm to individuals affected by the breach? *Refer to the Privacy Breach Assessment Tool*	☐ Yes ☐ No ☐ Unsure
8. Have the affected individuals been notified? *Consider your responsibility to notify individuals whose information has been breached. Prompt notification to individuals can help to avoid or lessen the damage by enabling the individual to take steps to protect themselves. Transparency and clear information about a breach is also important to help build trust.*	☐ Yes ☐ No ☐ Under consideration
9. What action, including remedial action, has been taken or is intended to be taken to contain and mitigate the impact of the breach?	
10. What action has been taken, or is intended to be taken, to prevent a reoccurrence of the breach?	
11. Is this assessed as a notifiable breach and will OAIC be notified?	☐ Yes ☐ No ☐ Under consideration
12. List any other data protection authorities, law enforcement bodies or regulatory bodies that you have or intend to, report this breach to	

ATTACHMENT C

PRIVACY BREACH ASSESSMENT TOOL

What to do if you have found a potential information breach.

If there is an immediate risk to a person's life, health or safety, call 000 now.

This self-assessment tool gives you a process to follow and suggestions for help and advice.

For assistance with dealing with a potential breach and the tool, refer to the people in your agency who handle information security or privacy, read the Office of the Information Commissioner's online guidance (OIC) or call the OIC's enquiries service on (07) 3234 7373.

Are you a government employee or contractor who has discovered a potential breach of your agency's data?

☐ **Yes - continue**

☐ **No – Stop; this tool is designed to help government staff dea with a possible breach of government-held information**

A government agency is a department, a local government, a public authority, a university or a hospital and health service. ('Your agency' includes a government agency contracting you to provide services).

If you are acting as an individual, you may have a privacy complaint. Alternatively, you may be concerned about information you have received. In either of these circumstances, start by contacting the relevant government agency.

Does the breach involve personal information?

☐ **Yes - continue**

☐ **No – Stop; this tool is about personal information**

See the OIC's guidelines about privacy breaches for advice about personal information.

If it involves personal information, it may be a privacy breach. Seek advice from the people dealing with privacy in your agency. You may have to act on any data breach. Seek advice from the people dealing with information security in your agency.

What type of harm might happen? (Identifying the type/s of harm will help you assess the risk.)

- physical
- identity theft
- loss of benefits
- loss of employment
- reputational, agency or person
- loss of access to information
- humiliation or loss of dignity
- financial
- emotional
- psychological
- discrimination
- other – please describe

What to do if you have found a potential information breach.

Is the breach likely to cause serious harm? (Each of these characteristics adds to the likelihood of serious harm.)

Seriousness (extent, depth and duration of harm)

- the breach may lead to imminent, irreparable physical, psychological or financial harm – **consider immediate action and notification**
- the harm might be costly – physically, personally or financially
- the harm would require sustained remedial action
- the harm is difficult to remedy
- the breach involves a combination of types of information
- the information is sensitive, for example, medical records

Likelihood (amount, dispersal and ease of access, and intent)

- harm has already occurred
- there is a risk of further access, for example online or via media
- the breach affects many people (also might increase seriousness)
- the breach occurred on multiple occasions or with other breaches (also might increase seriousness)
- the personal information is easily accessed, for example, was not encrypted or anonymised
- the information went to a person likely to cause harm, for example, if stolen or in a domestic violence situation

If you have a privacy breach and potential harm is:	
Not serious/ Unlikely No need to notify OIC	**Serious/ Unlikely** Consider notifying OIC
Not serious/ Likely No need to notify OIC	**Serious/ Likely** **Recommend notifying OIC**

Seek advice from people handling privacy or information security in your agency to help you answer these questions.

What steps have you taken to reduce the potential harm?

- **if the breach is from a computer system**, contact your computer / information systems team immediately (they may need to access or lock down the system and collect evidence)
- recover information before the information is accessed, for example, hard copy documents
- fix any non-computer related problems that caused the privacy breach, for example, securing rooms or cupboards
- contact the people who received the information to discuss mitigating harm, if that might help
- contact the people who may be affected to enable them to take immediate steps to minimise harm, for example to avoid or lessen the impact of disclosed financial information or contact details.

You may need to notify:

- **internally** in your agency, for example, your Program Manager or a designated person
- **externally** (for example, information security, the insurer, Police, OIC, OAIC) – seek advice from your agency

Consider your responsibility to notify individuals whose information has been breached. Prompt notification to individuals can help to avoid or lessen the damage by enabling the individual to take steps to protect themselves. Transparency and clear information about a breach is also important to help build trust.

Refer to OIC online guidance. Talk to people in your agency handling privacy or contact OIC's Enquiries Service on (07) 3234 7373.

What to do if you have found a potential information breach.		
Agency assessment record		
You may wish to expand this assessment record. **For example, you may wish to record details of the breach, details of action taken in response, any contact made for assistance, delegated decision-making authority, notification decisions, reasons for decisions.** **As a minimum, include the following details in this record.**		
Assessor's name/signature	Assessor's position	Date of assessment