SEARMS

Privacy, Confidentiality and Decision-Making Policy

ASES Standards	**Standard 2: Governance** • Requirement 2.3: Data and Knowledge Management Standard **Standard 6: Communication** • Requirement 6.1 Communication Standard **Standard 8: Consumer Outcomes** • Requirement 8.1: Consumer and Community Engagement Standard
Contractual Obligation(s)	NSW DCJ Specialist Homelessness Services (SHSs) Funding Agreement: Lead Entity and/or Joint Working Agreements
Related Policies	Case Management Communication Information Management Notifiable Data Breaches Professional Code of Ethics and Conduct Staff Induction

1. SCOPE

This policy applies to all employees, volunteers, students and consultants who are engaged to work with clients directly and who have access to information pertaining to clients.

2. PURPOSE

This policy provides guidance regarding how the organisation collects, uses, discloses and otherwise manages personal information. It also provides guidance regarding legal obligations and ethical expectations in relation to privacy and confidentiality.
The aim of this policy is to:

- Facilitate the provision of quality services for which information is collected, stored, used and disclosed in a manner that complies with both legislative requirements and ethical obligations.
- Inform all staff and Board members about their privacy and confidentiality responsibilities in relation to personal and organisational information about SEARMS its clients, staff, volunteers, students and stakeholders.

3. POLICY

SEARMS is committed to ensuring that information is used in an ethical and responsible manner and recognises the need to be consistent, careful and thorough in the way that information about clients, staff, Board members, students and volunteers[1] is recorded, stored and managed.
In terms of information, SEARMS:

- Collects personal information in private environments, as private as possible, to protect the privacy and dignity of individuals.
- Collects and uses personal information only to fulfil its functions and purposes, or for another acceptable reason with the relevant person's consent (unless exceptions covered in Section 6 in the Procedures Section apply); acceptable purposes for collection and use include:
    - For **clients**—service provision, referral, consultation, advocacy, reporting aggregate data for funding bodies, external audits and research
    - For **staff**, **volunteers** and **students**—recruitment, selection, employment, induction, payroll and tax, leave, supervision, development, performance management and review, and any other legitimate work-related purpose
    - For **consultants** and **contractors**—tendering, contract creation, monitoring and execution
- Ensures that all persons about whom personal information is being obtained are informed why the information is being collected and how it is and will be used, stored and administered.
- Stores personal information securely, protecting it from unauthorised access.
- Provides clients and other stakeholders access to their own information and the right to seek its correction.
- Provides information to clients about their rights regarding privacy in ways that clients find accessible and understandable to them.

SEARMS has a legal obligation to comply with the Privacy Act 1988 (Cwlth) and with the Australian Privacy Principles.
SEARMS respects clients' rights to acknowledge or refuse their consent for the various purposes it seeks to collect personal information and share information. Clients who acknowledge their consent for any purpose also have the right to withdraw their consent at a later time.
SEARMS documents clients' consent, which is preferably provided in writing. If clients give their verbal consent for any purpose, this must be recorded by the worker taking consent and then placed on file.
When a client refuses or withdraws his or her consent for any purpose that inhibits or prevents effective service provision, the implications of this should be explained and explored with the client—with the goal of overcoming any concerns that have led to the

[1] From here when the term 'volunteer' is used, it means or can mean client, volunteer, student, staff member, Board member or other stakeholders (e.g., consultants).

withholding of consent. The use of formal or informal advocacy may be helpful in such situations.

4. PROCEDURE

1. The Purpose of Collecting Information

SEARMS collects personal information if it is reasonably necessary or if it directly relates to the client's circumstances in the context of service provision.

2. Privacy Statement

After engaging with SEARMS, all clients receive a privacy statement. This is provided to them by/through the application process. The privacy statement includes the following:

- The purpose of collecting information.
- How the information will be used.
- The type of information that is collected.
- Limits to the privacy of personal information.
- How a client can access or amend his or her information.
- How a client can make a complaint about the use of his or her personal information.

3. How Information is Collected

SEARMS collects personal information through several different mechanisms, including:

- Client information management system (CIMS)
- Face-to-face meetings
- Telephone and email communications
- Case conferences

4. Type of information collected

SEARMS collects and holds personal information about a client when the information is relevant to providing services to the client. The type of information collected includes the following:

- client names, addresses and contact details
- intake, assessment and reassessment documentation
- client case management plans and plan revisions
- referrals to other agencies
- consent to collect and exchange information
- feedback and complaints from clients
- reports from other agencies
- case closure and service exit documentation.

SEARMS will only use client information for the purpose of service promotion when the client has provided written consent.

5. Collection Principles

The following principles guide data collection practice

- SEARMS will only collect information that is necessary for the performance and primary function of the organisation.
- SEARMS will explain to clients the purpose of collection and how the information is used.
- SEARMS will advise clients that any data collected are accessible to the individual.
- SEARMS collects personal information from the clients themselves whenever possible.
- If the information was collected from a third party, SEARMS will notify the clients and advise them the purpose of the collection.
- SEARMS will ensure that the client has provided consent to the collection of sensitive information. Sensitive information includes information about mental health, religious beliefs and ethnicity.

6. Pre-collection Tasks

Prior to entering information into the CIMS, it is important to complete the following:

- SEARMS will provide new clients the SHSs Charter of Rights and Responsibilities and ensure that the information in this document is explained to them. The Charter should be signed by SEARMS staff, and clients should also be asked to sign.

- SEARMS explains to each person the purpose of collecting data.
- SEARMS ensures that the CIMS levels of consent are explained to all new clients, and that consent is obtained.
- When clients have difficulty reading or speaking English, SEARMS takes the time to read the information to them and checks that they have understood the information. If there is doubt regarding whether the client has understood the information, the SEARMS worker will arrange interpreter services prior to requesting the client's signature.

7. Consent and Decision-making

A client's personal information should only be collected with his or her informed consent. When the client does not have the capacity to provide informed consent, personal information is collected through appropriately supported decision-making or substitute decision-making processes.

- **Informed Consent**

  Informed consent refers to advising clients of several matters before obtaining their consent. These matters include:
  - Why the information is being collected.
  - What will happen to the information being collected.
  - Clients' rights to be told about the support they will receive.

- What the likely outcomes of the support might be
- The provision of information to and from other services with which the clients are involved, or to which clients are to be referred.
- What the consequences are for the client (if any) if he or she does not provide the information.

- **Supported Decision-making**

If a person does not have the capacity to provide informed consent, and he or she has family, friends, advocates or other support people, then you should work with the person's informal network to assist him or her in a collaborative way. If needed, refer the person to an advocacy organisation. The NSW Government's publication, the Capacity Toolkit,[1] provides a framework that assists workers with the issues of capacity and consent in decision-making. The NSW Information and Privacy Commission has also developed the Privacy and People With Decision Making Disabilities Guide[2] to assist workers in this area.

- **Substitute Decision-making**

If the person has a formal guardian, with a current guardianship order, and if the order covers the areas of person's life that are in scope for service provision, then you should work with the guardian and the person to obtain necessary consent.
If you are still unsure if the person can provide informed consent, and he or she does not have support persons, advocates or guardians, then you should seek advice from the Guardianship Division of the NSW Civil and Administrative Tribunal.[3]

8. Collection Principles

The following principles guide data collection practice

- SEARMS will only collect information that is necessary for the performance and primary function of the organisation.
- SEARMS will explain to clients the purpose of collection and how the information is used.
- SEARMS will advise clients that any data collected is accessible to the individual.
- SEARMS will collect personal information from the client themselves whenever possible.
- If the information was collected from a third party, SEARMS will notify the client and advise why the collection was sought from that party.
- SEARMS will ensure that clients have provided consent for the collection of sensitive information. Sensitive information includes information about mental health, religious beliefs and ethnicity.

9. Pre-collection Tasks

Prior to entering information into the CIMS, it is important to complete the following:

- SEARMS will provide new clients the SHSs Charter of Rights and Responsibilities and ensure that the information in this document is explained to them. The Charter should be signed by SEARMS staff, and clients should also be asked to sign.

- SEARMS explains to each person the purpose of collecting data.
- SEARMS ensures that the CIMS levels of consent are explained to all new clients, and that consent is obtained.
  When clients have difficulty reading or speaking English, [EARMS takes the time to read the information to them and checks that they have understood the information. If there is doubt regarding whether the client has understood the information, the SEARMS worker will arrange interpreter services prior to requesting the client's signature.

10. Personal information integrity

SEARMS takes steps to ensure that the personal information collected, used and disclosed is accurate, current, complete and relevant.
SEARMS takes reasonable steps to protect the personal information it holds. These include steps against loss, interference, unauthorised access, modification or disclosure and other misuse of information. All information is protected by the following mechanisms:

- Locking filing cabinets and unattended storage areas.
- Physically securing areas in which the personal information is stored.
- Not storing personal information in public areas.
- Positioning computer terminals and fax machines so that they cannot be observed or accessed by unauthorised people or members of the public.
- Securely disposing, destroying or de-identifying information that is no longer required by the organisation.

The following technical safeguards are used to protect information:

- Using passwords to restrict computer access, with regular changes to passwords required.
- Establishing different access levels so that not all staff can view all information
- Using electronic audit trails.
- Installing virus protection and firewall software.

For more information, refer to the Professional Ethics and Code of Conduct Policy.

11. Access to Personal Information

Individuals have a right to access to personal information under the Privacy Act 1988 (Cwlth) and may request access to information held about them.
Situations in which access to information may be withheld include:

- Access may threaten the life or health of an individual.
- Access may leave an unreasonable effect on the privacy of others.

- The request is clearly frivolous or vexatious, or that access to the information has been granted previously.
- The information is relevant to existing or to anticipated legal proceedings.
- Denial of access is required, either by legislation or law enforcement agencies.

12. Authority to Exchange Information and Information Sharing

- **Confidentiality and Consent**

Information pertaining either to an individual or to the organisation is generally considered confidential. [Service Name] ensures that a client signs an 'authority to exchange information form' (or similar document) prior to releasing information to other persons or organisations, such as through referral to another service. The client's consent is sought for different types of information exchanges separately. The 'authority to exchange information form' will list each specific type of information to be exchanged, without generalisations. A client has the right to provide or refuse consent for each specific type of information that the organisation wishes to exchange. A client can also withdraw the consent that they had previously provided.

- **Reporting Non-identifying Information**

An organisation may be required to report to funding bodies, or to other government departments, on large scale. This generally involves non-identifying data collections (e.g., minimum data sets). When this is the case, a person's consent to share his or her data should not be taken for granted on the grounds that the data is non-identifying. Consent from the person should be sought—which can be refused or withdrawn—to participate in data collections of this nature.

- **Providing Access to Personal Information for Service Audits**

When an organisation undertakes accreditation against any service standards that involve external auditors reviewing client files, it should obtain client consent in writing. (However, this is unnecessary if client consent for this purpose was previously obtained.)

- **Sharing Information Without Consent**

Australian privacy legislation allows for sharing information without consent if failing to share information is believed to lead to certain risks. The disclosure of personal information without consent to government agencies, other organisations or individuals is permitted if:

  - It is authorised or required by law.
  - It is unreasonable or impracticable to seek consent.
  - Consent has been refused.
  - The disclosure is reasonably necessary to prevent or lessen a serious threat to the life, health or safety of a person or group of people.
  - The organisation is a mandatory reporter and it is legally obliged to release information to relevant authorities when making a report about a child who is believed to be at risk of significant harm.

The decision to share information without consent must be based on sound risk assessment and then approved by a Chief Executive Officer of SEARMS.

13. Professional Ethics and Code of Conduct

All staff are required to abide by the SEARMS Professional Code of Ethics and Conduct in relation to privacy and confidentiality.

14. Complaints

Clients have a right to make a complaint if they feel that there has been a breach of their personal information. SEARMS will:

- Inform clients of their right to make a complaint.
- Make the complaints procedure available to clients at the initial interview
- Log complaints about information handling in the complaints register and act to rectify problems.

15. Archiving and Destruction

SEARMS has a legal obligation to appropriately store and destroy information within time frames. For specific periods for the retention of information, refer to the Records and Data Retention Guidelines.

5. RESPONSIBILITIES

Responsibility	Delegation
Obtain consent to collect information	Chief Services Officer
Obtain consent to disclose information	Chief Services Officer
Secure storage of information	Chief Business Officer
Manage information	Chief Business Officer
Archive information	Chief Business Officer
Destroy information	Chief Business Officer

6. LEGISLATION

- Australian Privacy Principles

https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

- Privacy Amendment (Enhancing Privacy Protection) Act 2012

https://www.legislation.gov.au/Details/C2012A00197

- Health Records and Information Privacy Act 2002 (NSW)

http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/nsw/consol_act/hraipa2002370/

- Privacy Act 1988 (Cwlth)

https://www.legislation.gov.au/Details/C2018C00034

- Notifiable Data Breach Scheme

https://www.legislation.gov.au/Details/C2017A00012

7. APPENDICES

Appendix 1: Authority to Disclose Information
Appendix 2: SEARMS Privacy Statement
Appendix 4: SHS Charter of Rights and Responsibilities

8. FURTHER RESOURCES

- New South Wales Government. Capacity toolkit [Internet]. Attorney General's Department of NSW; 2008 [cited 2019, February].
- Information and Privacy Commission of New South Wales. Privacy and people with decision making disabilities guide [Internet]. 2004 [cited 2019, February]. Available from:

https://www.ipc.nsw.gov.au/privacy-and-people-decision-making-disabilities-guide

- Guardianship Division of the NSW Civil and Administrative Tribunal [Internet]. NSW Civil and Administrative Tribunal; 2020 [cited 2019, February]. Available from:

https://www.ncat.nsw.gov.au/Pages/guardianship/guardianship.aspx

VERSION	APPROVAL	EFFECTIVE DATE	REVIEW DATE
Version 001	Chief Business Officer	20 May 2024	20 May 2026