1 Purpose and Applicability

Southern Cross Care (WA) Inc (SCCWA) is committed to protecting the privacy of all personal and sensitive information collected from individuals including residents, clients or external service providers. SCCWA will ensure that personal information is managed and used in accordance with the Privacy Act 1988 (Cth), including the mandatory requirements contained in the Australian Privacy Principles - Schedule 1 of the Privacy Act.

All SCCWA staff, contractors, and volunteers are required to comply with this policy. All staff are responsible for ensuring that records and information containing personal and sensitive information are managed in accordance with this policy.

Privacy issues relating to SCCWA employee records are covered in the separate Employee Records Policy owned by the Chief People Learning and Culture Officer.

SCCWA's Privacy Policy will be kept up to date and in accordance with the requirements of the Australian Privacy Principles (APP) Guidelines endorsed by the Office of the Australian Information Commissioner. The APP are legally binding principles forming the foundation of the Privacy Act. The principles specify the standards, rights and obligations in relation to handling, holding, accessing, disclosing and correcting personal information.

Personal Information is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable. Examples include an individual's name, signature, address, telephone number, date of birth, etc.

Sensitive Information is a subset of personal information and includes:

- Information or an opinion (that is also personal information) about an individual's:
  - Racial or ethnic origin;
  - Political opinions / membership of a political association;
  - Religious beliefs or associations;
  - Philosophical beliefs;
  - Sexual preferences or practices; or
  - Criminal record.
- Health information about an individual;
- Financial information;
- Genetic information (that is not otherwise health information); or
- Biometric information that is to be used for the purpose of automated biometric verification or biometric identification.

Sensitive information is generally afforded a higher level of privacy protection than other personal information.

For the purposes of this document, reference to "Southern Cross Care (WA) Inc" encompasses the services provided by Southern Cross Care (WA), Southern Plus, Southern Plus Real Estate and Southern Cross Housing Ltd. This policy applies to Southern Cross Care (WA), Southern Plus Real Estate, Southern Plus and Southern Cross Housing Ltd.

2 Policy

SCCWA is committed to ensuring personal information is used, managed and protected in accordance with the Privacy Act 1988 and the Australian Privacy Principles. SCCWA's Privacy Officer role is undertaken by the Risk Manager, who will ensure this policy is reviewed at least once every three years and also when there is any change to the legislation or APP Guidelines.

References to "personal information" in this policy includes both "personal" and "sensitive" information unless stated otherwise.

2.1 Collection of information

As a provider of Aged, NDIS and Mental Health care, SCCWA collects and maintains personal information relating to our residents, clients and contractors engaged. SCCWA will collect only necessary personal and sensitive information which is required to perform core business functions.

Information is collected using only lawful means including directly from the individual or authorised delegate including current and/ or previous care provider.

SCCWA must ensure that the individual about whom the information is collected is aware of the following:

- That SCCWA has collected personal information that is required to perform our core business functions;
- How that information will be used and disclosed; and
- SCCWA's Privacy Policy.

2.2 Storage and safeguarding of personal and sensitive information

2.2.1 SCCWA strives to ensure the security of personal information collected and held in both electronic and hard form. SCCWA will take reasonable steps to protect personal information from misuse, interference, loss and from unauthorised access, modification, corruption and disclosure. The ICT Cyber Security Policy applies to personal information stored in electronic form.

2.2.2 When no longer required, SCCWA will take all reasonable steps to destroy and/ or de-identify the personal information once it is no longer required.

2.3 Use and disclosure of information

2.3.1 SCCWA will only use or disclose personal information for reasons which are consistent with the primary purpose, or directly related secondary purposes, for which it was collected, unless:

- The individual has consented to the disclosure; or
- SCCWA is required or authorised by Australian law or a court / tribunal order.

2.3.2 SCCWA will primarily use resident / client personal and sensitive information to assess an individual for suitability for admission; or provide a high level of appropriate care and services.

Resident / client personal and sensitive information will be routinely utilised by SCCWA staff and, if and when required, disclosed to external health care professionals (e.g. nominated GP, site pharmacist, etc.)

2.3.3 SCC may use personal and sensitive information to monitor the quality and effectiveness of services provided. As such, SCC, or its authorised delegate, may use personal information to request feedback on services provided.

2.3.4 SCC may disclose personal and sensitive information for administrative purposes, to meet legal and contractual obligations. For example, personal information may be disclosed to government agencies for funding and/or reporting purposes, or the health record may be subpoenaed.

2.3.5 SCCWA will take reasonable steps to ensure information disclosed for reporting purposes is de-identified where possible.

2.3.6 SCCWA may disclose health information about an individual for a secondary purpose to a "Responsible Person" if all of the following circumstances apply:

- The individual is either physically or legally incapable to provide consent to the disclosure;
- The disclosure is necessary to provide appropriate care, treatment or support of the individual, or disclosure is for compassionate reasons;
- The disclosure is not contrary to any wish/es expressed by the individual before consent could not be obtained, of which SCC is aware of or could be reasonably be expected to be aware of.

2.3.7 Residents and clients will be asked for consent to their personal and contact information to be used for general communication purposes at the time of admission. Consent may be withdrawn at any time.

3 Access, Disclosure and Correction

3.1 SCCWA will take all reasonable steps to ensure all information held is accurate, up to date, complete, relevant and not misleading. SCCWA will correct any inaccurate data as soon as reasonably possible on discovering that such information is inaccurate or misleading.

3.2 Personal information may only be disclosed to the individual who is the subject of that information, his/ her legally appointed representative, or to an individual or body that has legal authority providing entitlement to have that information.

3.3 An individual or their authorised representative may request access and/ or correct their personal information which SCCWA holds about him/her. SCCWA must respond to such requests within 30 days.

3.4 SCCWA will take all reasonable steps to meet the request, consult with the individual and provide access within 30 days unless there is a valid reason for not disclosing the information requested.

3.5 SCCWA may only refuse such access in exceptional circumstances including:

- Giving access would be unlawful;
- The information relates to legal proceedings between SCCWA and the individual and such information would not be accessible via the discovery process in legal proceedings;
- The request for access is frivolous or vexatious;
- Another valid reason exists for not disclosing.

3.6 The Freedom of Information Act WA 1992 does not apply to SCCWA. Personal information cannot be obtained via this Act. This legislation applies exclusively to WA Government and Local Government bodies.

3.7 There is no automatic next of kin right to personal or sensitive information, though such requests should be treated sensitively and in the context of the request.

3.8 There is no automatic next of kin right to financial information (including where the person seeking the information may be a beneficiary) unless the next of kin requesting the information has a valid legal appointment as executor or administrator, or some other legal authority for disclosure. In cases where the Public Trustee is appointed to administer a deceased estate, permission must be obtained from the Public Trustee prior to disclosure.

3.9 Resident/ client information may be accessed by a small number of authorised external agencies for the purposes of accreditation, funding etc. Requests must be made in writing and checked by the site manager to ensure that appropriate consent has been given for the release of such information. All such enquiries should be referred to site managers and/ or the Privacy Officer.

3.10 Some SCC clinicians may be bound by the Hippocratic oath as part of their registration as it relates to medical confidentiality and ethics.

3.11 In all scenarios covered in section 3 of this Policy, the Risk Manager in his role of Privacy Officer is available to discuss instances where it is considered that information should not be disclosed.

4 Data Breaches

4.1 SCCWA is required to take reasonable steps to protect the personal information held and has obligations under the Privacy Act 1988 (Cth) to put in place reasonable security safeguards and to take reasonable steps to protect the personal information held from misuse, interference and loss, and from unauthorized access, modification or disclosure.

Preventative and mitigating controls include but are not limited to:

- Identifying weakness in security profiles of technology across SCC and implementing strategies and steps to correct;
- Implementation of modern, robust authentication for external access;
- Review and align security password policies consistently across corporate applications and services; and
- Ensure appropriate management of hardcopy records through Induction Training and ongoing education.

4.2 A data breach occurs when there is unauthorised access to, or disclosure of personal information held by SCCWA. Data breaches are not limited to malicious actions, such as theft or 'hacking', but may arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure. All SCCWA employees. contractors and volunteers must notify their managers and the Privacy Officer of any actual or suspected breach.

4.3 Under the Privacy Act 1988 (Cth,) SCCWA must report to the Australian Information Commissioner breaches of certain private data likely to cause serious harm, unless remediation occurs before any serious harm results from the breach. All actual or suspected instances of data breach should be referred to the Privacy Officer/ Risk

Manager. When a data breach or suspected data breach has been identified, there are four main steps that SCCWA will undertake when responding:

1. Contain the breach and do a preliminary assessment;
2. Evaluate the risks associated with the breach;
3. Notify relevant parties;
4. Prevent future breaches.

Steps 1, 2 & 3 may be handled simultaneously or in quick succession.

4.4 The Privacy Officer/ Risk Manager will:

- Make a preliminary assessment and establish the occurrence and depth of breach in a reasonable and expeditious manner and at a maximum within 30 days of a breach being identified;
- Carry out an evaluation of risk and will establish the severity of the breach in terms of impact on person(s) where data has been breached;
- Notify parties affected upon the severity of the breach, data that has been breached or lost and impact on persons;
- Ensure that the risk of further breaches is reduced by adopting appropriate measures designed to prevent such breaches; and
- Take any further reporting measures necessary, e.g. in exceptional cases to the Office of the Australian Information Commissioner.

The Privacy Officer/ Risk Manager will decide the response to a breach on a case- by- case basis and may take additional steps if necessary.

5 Roles and Responsibilities

Role	Responsibility
Executive Management Committee	Endorse Privacy Policy
Privacy Officer	The privacy role is the responsibility of the Head of Risk
Heads of Departments and Managers	Manage and monitor compliance with this policy Ensure staff receive appropriate training and supervision to comply with this policy Ensure that operational decision making is informed by, and in compliance with this policy Report any privacy breaches to the Privacy Officer
All staff, contractors, temporary and voluntary staff	Comply with this policy Maintain knowledge of current practices as specified in this policy

6 Relevant Legislation and Guidelines

- The Privacy Act 1988 (Cth)
- The Australian Privacy Principles
- NDIS Practice Standards and Quality Indicators
- National Standards for Mental Health Services
- Aged Care Act 1997 (Cth)
- Aged Care Quality Standards

7 Other Relevant SCC Policies

Employee Records Policy

ICT Cyber Security Policy

8 Document Control

Rev	Owner	Sections Modified	Date Reviewed	Next Review Date
1.0	Head of Risk	First release	14/10/2022	13/10/2025