

Privacy Policy

Document reference:	Privacy Policy
Approved by:	St Simeon Healthcare Management
Date developed:	July 2024
Review Date History:	
Next Review Date:	July 2025

About this policy

This policy and process applies to all workers, contractors, volunteers and members of the board of St Simeon {we/us refers to St Simeon}. This Policy is written in plain language {you} refer to any individual about whom we collect personal information.

The specific legal obligations when collecting and handling residents' personal information are outlined in the Privacy Act and the Australian Privacy Principles (APPS) found in that Act.

Contents of this policy

About this policy	1
Contents of this policy	1
Legislative / Compliance Obligations	2
Associated documents	2
Introduction / background	3
Collection of Personal Information	3
Kinds of personal information we collect	4
Use and disclosure	5
Surveillance and use of CCTV	6
Anonymity	6
Overseas use and disclosure of personal information	6
Storage and security of personal information	6
How to access and correct your personal information	7
Privacy Officer Contact Details	7
Making a complaint about a breach of privacy	7
Notifiable Data Breaches Scheme (NDB Scheme)	8

Privacy Policy

Roles and responsibilities	9
Privacy and Confidentiality and the Current Aged Care Quality Standards	10
Privacy and Confidentiality and The Strengthened Aged Care Quality Standards	11
Policy statement	11
Risk assessment	11
Glossary	12
Evidence base	12

Legislative / Compliance Obligations

Aged Care Act 1997 is the main law that covers Government-funded aged care.

Aged Care Quality Standards and Guidance Materials 2019 & 2023

Australian Government and Aged Care Quality and Safety Commission Code of Conduct for aged care workers and governing persons

Aged Care Quality and Safety Commission Rules 2018

Draft Exposure Bill the Aged Care Act 2023

Health Records and Information

Privacy Act 2002

Privacy Act 1988 (amended by the Privacy Amendment (Private sector) Act 2000 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012)

Privacy and Personal Information Act 1988

User Rights Principles 2014

Quality of Care Principles 2014

Associated documents

Privacy and Confidentiality Process

Privacy and Confidentiality Consent Forms

Privacy Policy

Introduction / background

Privacy and confidentiality are fundamental principles that underpin trust, respect, and ethical conduct. These principles are essential for safeguarding resident, workers, and contractors' personal information, promoting autonomy and upholding their rights to control the disclosure of sensitive data.

We collect, hold, use and disclose personal information to carry out our obligations under the [Aged Care Act \(1997\)](#),

These responsibilities include:

- the quality of care we provide
- the user rights of people accessing care
- being accountable for the care provided.

We must:

- Protect the residents' privacy
- Comply with all applicable laws relating to the use of personal information
- Implement security safeguards to protect care recipients' personal information against loss or misuse
- Meet the Australian Privacy Principles in the [Privacy Act 1988](#)
- Meet obligations in state or territory privacy laws.

Protected information is information that was acquired under or for the purposes of the [Privacy Act 1988](#) and is personal information, as defined in the Privacy Act

Any unauthorised release or misuse of protected information is a breach of the Privacy Act and can result in personal penalties of up to 2 years imprisonment.

Collection of Personal Information

We collect personal information when you interact with us, and we perform our role as an Approved provider of Aged Care Services. For example, we may collect your personal information if you are a resident, a resident representative, an aged care worker, key personnel or a governing person.

We only collect the information we need for the function or activity we are carrying out. The main way we will collect your personal information is when you give it to us. For example, we collect your personal information when you:

- Contact us through the various contact channels we have (including phone, website, email and social media) to provide feedback or make an enquiry

Privacy Policy

- Speak to our workers when you visit one of our services
- Speak to our administrative or management workers
- Make, or provide information in connection with, a complaint about an aged care provider
- Submit a notification of an incident or reportable incident under the Serious Incident Response Scheme
- Give us information about your qualifications and experience in connection with an application for admission, commence a home care service
- Apply for a job with us

Sometimes we will collect your personal information indirectly, from:

- Your representative such as a legal guardian or family member
- Our website
- During the recruitment process
- My Aged Care Service Provider Portal at time of referral for service
- A third party, such as another government agency, where authorised by law or with your consent (if possible)
- An organisation contracted by us to provide services on our behalf or to assist us with its human resources, communications, IT or other corporate activities.

We will collect personal information through a range of different channels including when we communicate with you or your representative by letter, email, through our website and social media, when you respond to a survey in which you are identifiable and via the My Aged Care Service Provider Portal. We also collect personal information when you or your representative meet with us face-to-face or deal with us by telephone.

Kinds of personal information we collect

We collect a range of personal information where it is required for the exercise of our functions. The type of personal information we collect depends on the reason we are collecting it. The following kinds of personal and sensitive information are examples of personal information we may collect, where relevant to the function being exercised:

- Your name, address, date of birth, position title, gender and contact details (such as mobile phone number, address and email address)
- Other information to verify your identity, if required (such as country of birth, passport details, visa Details, driver's licence, birth certificates and ATM cards)
- Information such as banking details, your pension entitlements, and information regarding your income and assets. Where it is relevant to administer our payment arrangement, we will collect information such as your Medicare number, health care and your entitlement to government benefits. We use this information for arranging payment for your care and/or accommodation
- Information about your employment status and history, financial affairs, and your cultural and linguistic background
- Photographs, including clinical photographs of you or parts of your body (such as photographs of wounds)
- Information about your health and well-being, including any disabilities you may have

Privacy Policy

- Information about your preferences and wishes for your care (including care at the end of your life)
- Information about aged care services you need, or that are provided or needed by you
- Information about any family or other related persons such as partners, children, dependants, carers, and nominees or authorised representatives
- Information about criminal history (worker screening and key personnel)
- Records of our interactions with you such as letters, emails and notes
- Information about other healthcare professionals and health service providers who are involved in your care
- Information or opinions about your behaviour and treatment of aged care residents under the Code of Conduct (Workers' screening and Key personnel)
- Government identifiers (e.g. Centrelink Reference Number or Tax File Number)
- Information about how you use our online services such as online forms you fill in, pages you visit, your language preferences, and other online interactions including complaints or feedback.

If you send us your personal information when we don't ask for it we will determine whether the information is relevant to our functions. If it is not, we may destroy or de-identify the personal information if it is lawful and reasonable to do so.

Use and disclosure

We will generally only use and disclose personal information for the particular purpose for which it was collected. We may also use your personal information for a related purpose, such as to undertake our other functions or to survey you about your satisfaction with our service.

We routinely disclose personal information to a number of other agencies and bodies as required or authorised by or under law. We will not otherwise use or disclose your personal information for another purpose unless we obtain your consent, or the use or disclosure is permitted under the Privacy Act.

We may disclose personal information including health information about an individual to a person who is responsible for the individual if:

- The individual is incapable of giving consent or communicating consent.
- The St Simeon Healthcare Management is satisfied that either the disclosure is necessary to provide appropriate care or treatment is made for compassionate reasons or is necessary for the purposes of undertaking a quality review of our services (and the disclosure is limited to the extent reasonable and necessary for this purpose); and
- The disclosure is not contrary to any wish previously expressed by the individual of which the St Simeon Healthcare Management is aware, or of which the St Simeon Healthcare Management could reasonably be expected to be aware, and the disclosure is limited to the extent reasonable and necessary for providing care or treatment.

A 'Person Responsible' may, depending upon the circumstances, be a parent, a child or sibling, a spouse, a relative, a member of the individual's household, a statutory decision maker, guardian, an enduring power of attorney, a person who has an intimate personal relationship with the individual, or a

Privacy Policy

person nominated by the individual to be contacted in case of emergency, provided they are at least 18 years of age.

A 'St Simeon Healthcare Management' is a person employed by us in a management capacity and who is responsible for the provision of appropriate care and treatment of an individual.

Surveillance and use of CCTV

Inconsideration of the privacy and dignity of residents, St Simeon does not place recording devices such as security or surveillance cameras in residents' rooms or private spaces.

Signage will apply to areas subject to CCTV surveillance.

Anonymity

Whenever feasible, you have the option to interact with us anonymously or by using a pseudonym. This applies to situations such as making inquiries about programs, policies, or consultation procedures, as well as when submitting complaints.

In certain instances, maintaining anonymity or using a pseudonym may not be feasible, or we may be legally obligated to interact with you in an identified manner. For example, resolving a complaint may require us to collect your name. We will provide notification at the time of data collection if this is the case.

Overseas use and disclosure of personal information

We do not usually use or disclose personal information overseas, except in limited circumstances:

- Email traffic may be assessed by overseas service providers for malicious and harmful content, to mitigate security risks.
- We may send personal information offshore to the person the information is about or with the consent of the individual concerned. If we intend to disclose personal information to an offshore recipient in other circumstances, we will take reasonable steps to notify you.

Storage and security of personal information

Personal information held by St Simeon is stored on electronic media and on paper files. We take reasonable steps to protect your personal information against misuse, interference and loss, and from unauthorised access, modification or disclosure.

These steps include:

- Our workers undertake privacy training and attend privacy awareness and education sessions.
- Our networks and websites have security features in place to protect the information that we hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.
- Access to records by workers and contractors is restricted on a need-to-know basis.

Privacy Policy

- We restrict physical access to our office and areas housing personal information, use lockable cabinets, secure databases, permission restrictions and password protection.
- Emails you send to us are screened by our email security systems and may be viewed by authorised information technology personnel for security purposes.

When no longer required, we destroy or archive personal information in a secure manner and as permitted by relevant legislation.

How to access and correct your personal information

You have a right under the Privacy Act to access personal information that we hold about you. You also have a right to request correction of your personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading.

If you ask, we must give you access to your personal information, and take reasonable steps to correct your personal information, unless there is a law that allows or requires us not to. We will notify you in writing and explain our reasons if we refuse to give you access to, or correct, your personal information.

If you are seeking access to a resident's personal care and services file, including any administrative information, then the resident or their nominee can write to the Privacy Officer to request a copy of the file.

Once access is granted, we will provide you physical access to view your records as original records are not permitted to leave the premises, unless required by law. You can obtain a copy of your records, subject to any restrictions under the Australian Privacy Principles (APPS) in the Privacy Act. Physical access will always be accompanied by an authorised person of St Simeon. Access to personal records may be refused in limited circumstances including if your Medical Practitioner and we agree that access would affect your physical or mental health or put another person at harm.

If you wish to request access or correction of your personal information, you should contact the Privacy Officer using the details below.

Privacy Officer Contact Details

Email:	Info@stsimeon.org.au
Phone:	02 9675 3285 or 02 8645 4010
Address:	261 Hyatts Road Plumpton 2761

Making a complaint about a breach of privacy

We take the protection of your privacy seriously. Any worker, contractor, key personnel or governing person who breaches a resident's privacy will be subject to disciplinary process. We encourage feedback or complaints. In the first instance we encourage you to raise these issues directly with the St Simeon Healthcare Management. Alternatively, please lodge your complaint to the Privacy Officer listed above.

Privacy Policy

If you think we have not dealt with your concerns or complaints satisfactorily you can contact the Office of the Australian Information Commission (OAIC) to lodge a written complaint. There is more information OAIC website www.oaic.gov.au

Office of the Australia Information Commissioner

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: GPO Box 5218

Sydney NSW 2001

Notifiable Data Breaches Scheme (NDB Scheme)

The NDB Scheme applies to entities that have obligations to protect the personal information they hold under the *Privacy Act 1988* (Cth) (Privacy Act). The NDB Scheme requires entities to report eligible data breaches (breaches that are likely to result in serious harm) to the Office of the Australian Information Commissioner (OAIC). We are also required to notify affected individuals when a data breach is likely to result in serious harm to an individual whose personal information is involved.

A data breach occurs when personal information is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person.

The notification to individuals must include recommendations about the steps they should take in response to the data breach. We will notify the OAIC using the online [Notifiable Data Breach form](#).

For more information, see [Report a Data Breach](#).

Roles and responsibilities

Role	Responsibilities
Care Staff Employees (CSEs) (Care workers and all ancillary workers)	Care workers in aged care must respect older individuals' privacy by only sharing necessary information, obtain permission before sharing personal details, keep sensitive information confidential, follow organisational policies, maintain professional boundaries, stay updated on privacy practices through training, and treat older individuals with dignity and respect. These responsibilities help create a secure and trusting environment for older individuals receiving care. They do not enter a resident's private space with consent and ensure any discussions and materials related to personal or sensitive information are kept private. They attend training as required.
Team Leaders/ Supervisors (RNs/ Department Heads)	Registered Nurses (RNs) in aged care are responsible for safeguarding personal information, obtaining consent before sharing data, complying with privacy laws and organisational policies, maintaining professional boundaries, and educating Care Workers on privacy practices. Their role is crucial in upholding privacy standards and ensuring confidentiality in care settings. They do not enter a resident's private space without consent and ensure any discussions and materials related to personal or sensitive information are kept private. They supervise the team to monitor that workplace practices adhere to these requirements. They attend training as required.
Managers	Managers in aged care are responsible for overseeing and enforcing privacy policies, ensuring workers' compliance with privacy laws and regulations, conducting regular audits to assess privacy practices, addressing privacy breaches promptly, and providing training and guidance to staff on privacy protocols. Their role is vital in creating a culture of privacy awareness and upholding confidentiality standards within the organisation. They attend training as required.
Senior Leadership / Executive	Senior leadership in aged care is responsible for setting the tone for privacy and confidentiality practices, establishing a culture of privacy awareness, ensuring that privacy policies align with legal requirements, providing resources and support for privacy initiatives, and holding the organisation accountable for maintaining high standards of privacy protection. Their leadership is essential in promoting a commitment to privacy and confidentiality throughout the organisation.
Management / Board of Directors	Accountable to fulfil all legislative and regulatory requirements related to Privacy.

Privacy Policy

All workers are required to carry out their duties in accordance with their job descriptions, with the knowledge and skills attained as part of their profession or any qualifications, and in accordance with the Code of Conduct for Aged Care or St Simeon's Code of Conduct, practice or standards expected by St Simeon. Workers are expected to engage with residents appropriately and respectfully and to maintain professional boundaries.

Workers that do not have a universal professional code of practice or standards tied to their role, e.g. personal care workers, are subject to codes of behaviour or practise relevant to their role under their terms of employment.

Workers who are subject to professional standards (e.g., medical, nursing and allied health professionals), will have a higher threshold of professional training and qualifications, knowledge and skills, and scope of practice, and hence a higher threshold of conduct expected.

The content of professional standards varies but may relate to:

- The manner in which a resident is treated (including their rights to privacy and dignity);
- The need for tailored, frequent and clear communication with a resident
- Ensuring informed consent and good record keeping.
- Providing culturally appropriate care; and
- Providing quality care and services.

Privacy and Confidentiality and the Current Aged Care Quality Standards

Standard	Requirements
1 Resident dignity and choice	(3) (a) (b) (c) (d) (e) (f)
2 Ongoing assessment and planning with residents	(3) (a) (b) (c) (d) (e)
3 Personal care and clinical care	(3) (a) (b) (c) (d) (e) (f) (g)
4 Services and supports of daily living	(3) (a) (b) (c) (d) (e) (f) (g)
5 Organisations Service Environment	(3) (a) (b) (c)
6 Feedback and Complaints	(3) (a) (b) (c) (d)
7 Human Resources	(3) (a) (b) (c) (d) (e)
8 Organisation Governance	(3) (a) (b) (c) (d) (e)

Privacy Policy

Privacy and Confidentiality and The Strengthened Aged Care Quality Standards

Standard	Outcomes
1 - The Person	1.1, 1.2, 1.3, 1.4
2 - The Organisation	2.1,2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10
3 - The Care and Services	3.1, 3.2, 3.3, 3.4
4 - The Environment	4.1a, 4.1b, 4.2
5 - Clinical Care	5.1, 5.2, 5.3, 5.4, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.6, 5.4.7, 5.4.8, 5.4.9, 5.4.10, 5.4.11, 5.4.12, 5.4.13, 5.4.14, 5.5.15, 5.4.16, 5.5
6 - Food and Nutrition	6.1, 6.2, 6.3, 6.4
7 - The Residential Community	7.1, 7.2

Policy statement

St Simeon takes its obligations under the *Privacy Act 1988* and the *Privacy and Personal Information Act 2012* seriously and will take all reasonable steps in order to comply with the Act and protect the privacy of personal and sensitive information that we hold.

St Simeon ensures that the following elements are implemented throughout all operational practices:

- Compliance with relevant legislation, regulations and industry standards concerning privacy and confidentiality
- Full transparency with all individuals about how their personal information is collected, used, and disclosed. St Simeon ensures informed consent is obtained before accessing or sharing any sensitive data.
- Robust security measures including access and data protection protocols to safeguard personal information from unauthorised access, loss or misuse
- Established clear processes for reporting and responding to privacy breaches prompt, ensuring the appropriate actions are taken to mitigate risks and protect individuals' rights

St Simeon is committed to regular review and updating of privacy and confidentiality practices through audits, organisational education sessions, and feedback systems to maintain an organisation-wide level of privacy awareness.

Risk assessment

Risk category	Likelihood rating	Impact rating	Total risk score
---------------	-------------------	---------------	------------------

Privacy Policy

--	--	--	--

Refer to Risk Management policy.

Glossary

Privacy

Privacy is the right of individuals to control access to their personal information and decide how that information is collected, used and shared. It involves maintaining boundaries and protecting sensitive data from unauthorised disclosure.

Confidentiality

Confidentiality is the obligation to keep sensitive information shared by individuals private and secure, preventing unauthorised access or disclosure. It involves maintaining trust by respecting the privacy of personal details disclosed in confidence.

Closed-circuit Television (CCTV)

This means a television system that transmits images on a 'closed loop' basis, where images are only available to those directly connected to the transmission system. The transmission of closed-circuit television images may involve the use of coaxial cable, fibre-optic cable, telephone lines, infra-red and radio transmission systems. A hand-held or fixed video cassette recorder is not included in this definition unless it is connected to a transmission system.

Person Responsible

May, depending upon the circumstances, be a parent, a child or sibling, a spouse, a relative, a member of the individual's household, a statutory decision-maker, a guardian, an enduring power of attorney, a person who has an intimate personal relationship with the individual, or a person nominated by the individual to be contacted in case of emergency, provided they are at least 18 years of age.

Evidence base

Aged Care Quality and Safety Commission (2018) Act, Rules, and Code of Conduct

Aged Care Quality and Safety Commission (2019 & 2024) Aged Care Quality Standards and Guidance Materials

Australian Government | Department of Health and Aged Care (2020) Privacy and Confidentiality Flyer

Australian Government | Department of Health and Aged Care (2024) Responsibilities of approved aged care providers

Australian Government (1988) Privacy Act

Australian Government (1998) Privacy and Personal Information Act

Australian Government (2002) Health Records and Information

Privacy Policy

Australian Government (2014) Quality of Care Principles

Australian Government (2014) User Rights Principles