Policy: Privacy (public)

Version: 04 January 2024

Contents

If you need a translator or interpreter, please contact TIS National on 131 450.

In this Policy, when we use ***we, us* or *our***, we are referring to
St John Ambulance Western Australia Limited and Apollo Health Ltd (together **St John WA**),
our head office is at 209 Great Eastern Highway, Belmont, Western Australia 6104.

When we use **you or your**, we are referring to **the reader** as an individual.

1. Purpose

The purpose of this policy is to explain how St John WA complies with the *Privacy Act 1988* (Cth), including the 13 Australian Privacy Principles (APPs). Our *Privacy Code of Practice* sets out our roles and responsibilities under the APPs in more detail.

Under Australian Privacy Principle 1 (APP1), we are required to have a clearly expressed and up to date privacy policy about how we manage personal information.

You can find out more about the *Privacy Act 1988* (Cth) and how it applies to you on the Office of the Australian Information Commissioner website – ***www.oaic.gov.au***.

2. Scope

This policy applies to all St John WA employees, volunteers, contractors, and any other representatives of St John WA. The scope is limited to our obligations under the *Privacy Act 1988* (Cth) (referred to in this document as *Privacy Act*) and any other legislation relevant to the protection of personal and sensitive information.

2.1 Who we are

St John WA's purpose is to serve humanity and build resilient communities through the relief of sickness, distress, suffering and danger. St John WA supports the wellbeing of our local communities by providing services such as the State Operations Centre (000 calls), ambulance, patient, and community transport services, first aid training, equipment and products, event health and industry medical services, urgent care centres, general practice, and dental services, as well as the first responders program across Western Australia. St John WA team members can be employees, volunteers, or contractors.

3. Principles

3.1. What is personal information?

In the *Privacy Act,* **personal information** is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.'

The term 'personal information' covers a broad range of information including:

- **General information** – your identity (name, age, date of birth, sex, marital status), contact details (residential / mailing address, email, telephone number, next of kin etc) and financial details (for payment of services).
- **Sensitive information** – includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, or criminal record, provided the information or opinion otherwise meets the definition of personal opinion.
- **Health information** – any personal information about your health or disability such as medications and medical history (this might include sensitive information).

Employee record information – current and former employee records are exempt from the *Privacy Act 1988* (Cth), however records kept during the recruitment process are personal information. Employee records are

held under the *Fair Work Act 2009* and *Fair Work Regulations 2009*. For more information on your rights, please see the Fair Work Ombudsman website – *www.fairwork.gov.au*.

Information can be in any form, including voice recordings, photographs, biometrics, location information from a mobile device, tissue samples, as well as traditional written and digital formats.

3.2. What is de-identified information?

De-identified information is when personal information has gone through a process to remove or alter it so that individuals can no longer be identified.

Generally, de-identification involves two steps:

- removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

We may de-identify information for secondary business purposes such as research or where it is no longer required for the primary purpose for which it is collected.

3.3. Can I be anonymous or use a pseudonym?

The *Privacy Act* allows individuals to ask to be anonymous or to use a pseudonym (fake name) instead of giving personal information. Due to the nature of emergency and health services we provide, there are very limited situations, such as when you provide feedback through our website or telephone us to a make a general enquiry, where you will be able to be anonymous or use a pseudonym. However, if you have a specific requirement, such as for your safety in a family or domestic violence situation, please contact us.

3.4. What about consent?

Under the *Privacy* Act, we must collect personal information in a lawful and fair way and that includes asking for consent, where practicable to do so. You can withdraw your consent to us collecting your personal information at any time, however this might make it more difficult for us to provide our services to you.

In a situation where there is a serious threat to your life, health, or safety, we may collect personal information, such as your name and contact information, and sensitive information such as health information, without your consent so that we can provide emergency health services to you.

If practical, we will collect the personal information directly from you but there are situations where this might not be possible, for example:

- if you are unconscious or unable to communicate, we will provide emergency health services to you.
- if you cannot understand us, we may ask an interpreter to help us communicate with you.
- if you are a minor, we may ask a parent or guardian.
- if you have a physical or mental impairment, we may ask a carer or guardian.
- if you are temporarily incapacitated, we may ask a responsible person to assist us.

We will need to provide your personal information, including any sensitive and health information we have collected, when we hand over your care from our service to another health service provider to assist with your ongoing treatment. We may be unable to obtain your consent at the time to do this.

There are permitted general situations under the *Privacy Act* where we may collect or disclose personal, including sensitive and health information, without your consent, such as where there is a serious threat to your life, health, or safety; to locate a missing person; if unlawful activity or misconduct of a serious nature is suspected; during a confidential alternative dispute resolution process; or defending a legal or equitable claim.

There are also rules under the *Privacy Act* which allow health information to be collected if it is required or authorised by or under another Australian law or is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind us. An example of this is when we collect information to include in your My Health Record under the *My Health Records Act 2012* (Cth) if you as an individual have opted into My Health Records and provided access rights for us to do so.

If you are concerned about what information has been collected and disclosed, without your consent, please contact us.

For more information about your rights under the *Privacy Act 1988* (Cth) in relation to health services, please see the Office of the Australian Information Commissioner website – *www.oaic.gov.au*.

3.5. Why do we collect, use, hold or disclose your personal information?

We collect, use, hold (store) and disclose (provide to others outside St John WA) personal information if it is reasonably necessary for one or more of our business functions, services, or activities and where required or authorised by law or court/tribunal order. These include:

- 000 State Operations Centre
- emergency ambulance services
- emergency and non-emergency health services
- patient transport and community transport services
- first aid training and services, including school programs and youth services
- medical and first aid services to private clients at public and private events
- industry medical services provided to organisations
- urgent care services
- general practice, medical, medical specialist, pathology, and allied health services
- dental and emergency dental services
- digital services including the First Responder App, online first aid community training
- community engagement activities including school programs
- volunteer opportunities and services
- recruitment, employment, and training services
- stakeholder and relationship management
- fundraising, donations, and related charitable activities
- media engagement, marketing, general promotional activities, and surveys
- goods and services transactions
- billing and insurance claims
- internal reporting for evaluation, monitoring, and service improvement
- evidence-based policy planning
- governance, legal and statutory regulation obligations
- reporting to the WA Department of Health and other funding bodies and stakeholders
- providing information for referral to health professionals, health, and other service providers
- research or statistical activities relevant to public health or for the management, funding or monitoring of a health service
- any other services to improve the wellbeing of the community.

We provide real time and historical personal information to our main funding body, the WA Department of Health, as part of our contractual obligations in providing ambulance, non-emergency patient transport and other funded services to the community of Western Australia.

We also provide personal information to assist law enforcement agencies, such as the Western Australia Police Force, the Coroner, courts, tribunals, and statutory agencies. We work with universities and research bodies on medical research projects, which may involve sharing personal information.

3.6. What kinds of information do we collect and hold?

We collect a broad range of personal information from you, some of which may include health information, employee record information, financial information, and sensitive information. For example, we may collect personal information such as your name, address, and other information specific to the service provided to you or the business relationship you have with us.

The personal information we collect, and hold is necessary for one or more of our business functions, services, or activities. For example, we may collect:

- health information, health insurance, Medicare, and financial information from you when you use our emergency ambulance services, patient transport services or attend one of our urgent care, general practice, or dental centres,
- your financial information when you buy first aid equipment from us or pay for first aid training or make a donation,
- employment and volunteer application, qualification and licences, health information and financial information to manage our recruitment processes,
- personal information from you when downloading our First Responder App to access resources and services via the App and to act as a First Responder in the community.

Further detailing on collection, use and disclosure for different service offerings and activities are contained in privacy collections statements for those services or activities.

We generally collect sensitive information about you where it is directly related to one or more of our functions or activities listed in 3.5 and only with your consent. However, we may collect sensitive information without your consent - where it is required or authorised by law; to lessen or prevent a serious threat to life, health, or safety; to take appropriate action against suspected unlawful activity or serious misconduct; to locate a missing person, establish or defend against a legal claim; or for a confidential alternative dispute resolution process.

We may hold your personal information in a number of ways including:

- in our websites, computer systems or databases
- in paper records, and / or
- in social media or surveys.

3.7 How do we collect personal information about you?

We generally collect personal information directly from you where practicable, however there are times when we may not be able to do this, such as when you are unconscious, unable to communicate or do not have legal capacity. In these situations we may ask someone who can act on your behalf, or a responsible person, to provide us with your information.

We may collect and receive information about you from third parties, such as when your friends or relatives call 000; from other health, medical or allied care or support services; or from insurance companies or government agencies in relation to the services we provide to you. We may also receive information from your health insurance fund, Medicare, or other funding body to help us manage your account.

3.8. What about the internet?

We may collect information about your visit to our website and use cookies to assist us to measure and improve how we provide services and information on the internet. Cookies are small information files that an

end user's web browser places on their computer when a website is visited. For information on disabling cookies, please go to the privacy settings within your web browser.

We retain the content and associated data of any online messages, surveys, and emails (and any attachments) that you send to us, if we believe we have a legal right to do so. Your email message may be monitored by us and our response to you may also be monitored for security and quality assurance issues.

3.9 What about direct marketing ?

We provide services for the benefit of the community and may use personal information for direct marketing purposes to inform you of our services and products, for fundraising activities and appeals. As a registered charity, we are exempt from the *Spam Act 2003* and the *Do Not Call Register 2006,* but we comply with the APPs in our direct marketing and fundraising efforts.

We will follow the obligations set out in any relevant legislation, including the *Telecommunications (Telemarketing and Research Calls) Industry Standard 2017* in relation to marketing and promotional communications.

St John WA adhere to the *Fundraising Institute of Australia Code*, a voluntary, self-regulatory code of conduct for fundraising in Australia which is informed by the International Statement of Ethical Principles in Fundraising.

You can opt out of receiving direct marketing communications from us by using the unsubscribe option in any emails, or submitting a feedback or complaint form, or contacting us by phone or email – *https://stjohnwa.com.au/about-us/contact-us*.

3.10 Do we send information overseas?

We will only disclose your personal information for the purpose for which it is collected and with your consent, unless authorised by law to do so, or in the interests of your immediate health and safety.

Whilst we try to keep patient and client data within Australia, the nature of cloud computing means that some of our systems may transfer information overseas. We put in place security measures, such as access control and encryption, to reduce the risk of information being misused or interfered with.

We will ask the overseas recipient (organisation or person we are sending information to) to comply with the Australian Privacy Principles if the country they are in do not have a similar law or binding scheme as the *Privacy Act*.

St John WA are part of the Order of St John, whose head office is in London, England. We provide personal information of Order members (or Members of St John WA company) to St John International, who are the supporting body for all St John organisations.

If you have any concerns about how your personal information will be disclosed, please contact us.

3.11 What is unsolicited personal information?

Unsolicited personal information is personal information that we have not asked for. If we receive any unsolicited information that is not reasonably necessary, or directly related to one or more of our business activities, then we will de-identify or destroy it as soon as practicable.

If you receive information from us that is not meant for you, please delete it immediately and contact us to let us know.

3.12 What about security measures?

We will protect your personal information as far as practicable from misuse, interference, loss, and from unauthorised access, modification, or disclosure. We do this by using security measures in our information

communication and technology systems. We require that our employees, volunteers, and contractors follow policies and procedures regarding accessing information and systems. We use multifactor authentication to reduce the risk of unauthorised access and we monitor our systems for security threats.

We also use third-party solutions or providers to collect, process and hold information, depending on our business activities. In these instances, we take reasonable steps towards ensuring protection of personal information shared, including assessment of the security arrangements and controls of third-party providers.

If we hold personal information that is no longer needed for one of our business activities or functions and we are not required by law to retain it, we will de-identify and / or destroy it. We may need to keep health information for longer than other personal information in order to meet our contractual and legal obligations.

If there is unauthorised access or disclosure of personal information which is likely to result in serious harm to you, and we have been unable to prevent this, we will notify you and report the breach to the Office of the Australian Information Commissioner under the Notifiable Data Breach Scheme. You can find out more about the Scheme on the OAIC website – www.oaic.gov.au.

4. Accessing and correcting your personal information

We aim to ensure that the personal information we hold is accurate, up to date, complete, relevant, and not misleading. Under APPs 12 and 13 you have the right to ask for access to personal information that we hold about you, and to ask that we correct that personal information.

If you would like to seek access to, or revise your personal information, or feel that the information we hold may be incorrect or incomplete, please contact us.

We aim to respond to you within 30 days of your initial request.

To access your patient records, you will need to email us at *compliance@stjohnwa.com.au* and complete our *Request to Access Patient Records Form*. There may be a charge for this.

To ensure your personal information remains accurate, up-to-date, complete, and relevant, please email us at *compliance@stjohnwa.com.au* to make any necessary corrections. There is no charge for requests to correct your personal information.

We will ask you to verify your identity before we give you access to your information or correct it.

If we are unable to correct your information on the original record due to legal or contractual obligations, we may be able to add a statement instead. If we are unable to give you access to, or correct, your personal information, we will tell you of the reasons why. We will also take reasonable steps to inform any third parties of your request.

We may not provide access to your personal information where exempted from doing so under the APP 12, including where doing so will:

- pose a serious threat to the life, health, or safety of any individual or to public health or safety;
- have an unreasonable impact on another person's privacy;
- prejudice the taking of appropriate action relating to suspected unlawful activity or serious misconduct;
- prejudice an enforcement body from conducting enforcement related activity;
- affect a commercially sensitive decision-making process;
- affect an existing or anticipated legal proceeding;
- denying access is required or authorised by law or a court/tribunal order.

5. How do I make a complaint?

If you believe that we have breached your privacy in our handling of your personal information, you may lodge a complaint with us. Our complaints, feedback and compliments forms are available on our website at *www.stjohnwa.com.au/about-us/contact-us/feedback*.

If you are unhappy with the resolution of your complaint, or the way we have handled your complaint, you may refer your complaint in writing to the Office of the Australian Information Commissioner by email to *enquiries@oaic.gov.au* or see their website for more contact details – *www.oaic.gov.au*.

6. Contact us

If you are concerned about your privacy and would like further information, please contact us. Please make a general enquiry before providing us with copies of any personal information, sensitive or health information as we may not need this to answer your query or deal with a request.

This policy is currently available in English PDF format and on our website. Please contact us if you need this policy in a different format.

Email: Privacy Officer – *feedback@stjohnwa.com.au*

Tel: (08) 9334 1222 (Mon-Fri 8.30am – 4.30pm)

Mailing Address: PO Box 183 Belmont, Western Australia 6984

Please visit our website at **www.stjohnwa.com.au** and **www.stjohnhealth.com.au** for more contact information, to connect with our primary health services and details of our regional offices.

7. Policy Administration

Roles and Responsibilities

Role	Specific Responsibility
Privacy Officer	Maintain and update this Privacy Policy in accordance with the *Privacy Act 1988* (Cth)

Related documents

Information Management Framework
Information Management Policy
Privacy Code of Practice

Commitment to Privacy (public)

As the Group CEO, I endorse our organisation's Privacy Policy, reaffirming our commitment to privacy principles, processes, and our obligations under the *Privacy Act 1988* (Cth) to safeguard personal and sensitive information.

All team members have a personal responsibility to ensure good privacy practices and compliance with the Group's Privacy Policy and processes in managing personal and sensitive information.

Thank you for joining me in this commitment to privacy.

Kevin Brown

Group Chief Executive Officer

Policy Administration					
Policy Name:	**Privacy (public)**			**Policy No:**	**IM-LEG-01**
Policy Owner:	Legal Department			**Responsible Manager:**	General Counsel
Risk Rating:	Medium			**Review Cycle:**	Annual
Interdepartmental Relationships	**Name**				**Date**
Consulted with:	Information Management Steering Group				25/10/2023
Informed:	Risk, Compliance and ESG Committee				07/11/2023
Policy Approver: Group Chief Executive Officer					
Date of Approval:	04/01/2024				
Date of Review:	01/2024	**Due Date of Next Review:**	01/2025	**Version No:**	3
Compliance References					
Statutory:	*Privacy Act 1988 (Cth)*				
Industry:	n/a				

Version History		
Version	**Description of Change**	**Author**
1	New Policy	Unknown
2	General review – March 2021	Head of Legal
3	Update to reflect *Privacy Act 1988* (Cth) Australian Privacy Principle 1 – open and transparent privacy policy and external consultant recommendations.	Data Governance Lead / Privacy Officer