Privacy

Overview

St George Community Housing and its subsidiaries (we, our and us) respect the privacy of customers and are committed to meeting all obligations under relevant privacy laws, including the Privacy Act 1988 (Cth) (Privacy Act) and the Australian Privacy Principles (APPs). This policy outlines how we handle personal information and meet our legal duties.

Scope

This policy applies to all personal information collected, received, used, disclosed and held by us.

Definitions

Personal Information

Personal information means 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 material form or not.

Typical examples of personal information include a person's name, address, telephone number, bank account details or credit card information.

Sensitive Information

Sensitive information is a subset of personal information that is afforded higher levels of protection under the Privacy Act. It includes information or opinion about an individual's racial or ethnic origin, political opinion, membership of a political association, professional or trade association or trade union, religious beliefs, sexual orientation, criminal record or health information.

Types of information we hold

In order to provide services to our customers, we often need to collect personal information. We might hold personal and sensitive information about a person including their name, postal, residential and email address, gender, date of birth, nationality, language/s spoken, education and qualifications, bank account details, proof of identity, photographs, health or medical information and emergency contact details.

Collection of personal information

We might collect personal information and sensitive information when it is reasonably necessary for one or more of our functions or activities related to the delivery of our functions, such as:

- Communicating with customers about our products/services
- Processing applications for housing
- Managing tenancies
- Service improvement
- Service delivery reporting
- In the course of providing our services and responding to inquiries from government departments in connection with the services we provide

We might collect personal and/or sensitive information from a person when they:

- Fill out a form

- Call or video conference us
- Email us
- Visit our website
- Visit our office/s
- Use an IT device we provide

Where possible, we will collect personal information about a person from the person. However, there may be times we receive information about a person from third parties or publicly available sources or through other agencies that we deal with. We might also receive personal information that we have not requested (unsolicited information). If we receive unsolicited personal information, we will determine if we could have collected the information under privacy laws. If we determine that we could not have collected the personal information, we will destroy or de-identify the information. If we determine that we could have collected the information (or if the information is contained in a Commonwealth record or it would be unlawful or unreasonable to destroy or de-identify it), then we may keep the information and we will comply with our legal requirements in relation to the information (e.g. notification of collection, use and disclosure, storage and protection, access and correction).

Where it is practicable and legal, we will let people remain anonymous or use a pseudonym (a name that is not their legal name) to communicate with us, for example, if you contact us to ask a general question. However, we will usually need your name and contact information to be able to respond to questions and requests.

Use and disclosure

We will only use or disclose personal information that we hold for the purpose which we collected it for (the primary purpose), or for a related purpose (or a directly related purpose for sensitive information), unless:

- The person has given us permission to use or disclose it for another (secondary) purpose
- The person would reasonably expect us to use or disclose the information for another (secondary) purpose
- The use or disclosure is required or permitted under Australian law or by a court or tribunal order
- We reasonably believe that use or disclosure is reasonably necessary for enforcement related activities (including the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities)
- We reasonably believe that use or disclosure is needed to reduce or prevent a serious threat to the life, health or safety of any person, or to public health or safety
- For any other legal purpose.

We might collect, use, or disclose government related identifiers, such as a driver's licence or Centrelink Reference Number (CRN), in accordance with APP 9 where we need the information for our functions or activities. For example, we may need to use and/or disclose a government related identifier to verify an individual's identity or to fulfil our contractual obligations to an agency or State authority.

Storage and protection of personal information

We store personal information in both hard copy and electronic form. We will take all reasonable steps to make sure that personal information is stored securely and is protected from misuse, interference or loss and unauthorised access, modification or disclosure. If

information we hold is part of an eligible data breach, we will meet our obligations under the Notifiable Data Breaches Scheme.

As a general rule, we will not disclose personal information to any recipients outside Australia. However, some personal information we hold electronically might be stored overseas using cloud computing or other electronic storage services. Where we store personal information overseas and it is a disclosure under the APPs, we will take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.

If we hold personal information about an individual and we don't need the information anymore or we aren't legally required or authorised to keep the information, we will take all reasonable steps to destroy or de-identify the information.

Access to and correction of personal information

We will take all reasonable steps to make sure the personal information that we collect, hold, use and disclose is accurate, up to date, complete and relevant.

Individuals are welcome to request that we provide access to the personal Information we hold about them by contacting us using the details listed at the end of this Policy. Generally, we will provide access to the information in the manner requested unless applicable laws allow us to refuse, or prevent us from giving, access to the personal Information. We will not unreasonably refuse requests to access personal Information and we will respond to requests for access within a reasonable time.

Where we agree to provide access to personal Information, we may make this conditional on us recovering our reasonable costs of doing so from the person seeking access. No fee will be incurred for requesting access, but if a request for access is accepted, the individual will be notified of the fee payable (if any) for providing access if they proceed with the request.

Individuals may also lodge a request to correct personal Information we hold about them if they believe it is inaccurate, incomplete, irrelevant, misleading or out of date. There is no fee for doing this. To do so, please contact us at the contact details listed at the end of this Policy.

If we aren't satisfied that the personal information should be changed, we will provide the person with a written notice explaining the reasons for our decision and how they can make a complaint if they aren't happy with our decision. If we refuse a request to change personal information, the person can ask us to attach a statement to the record stating that the information is inaccurate, out-of-date, incomplete, irrelevant, or misleading.

Privacy and our website

Web analytics

We use Google Analytics to collect data about the way people use our website. We use the information collected to help to improve our website. Google Analytics is hosted overseas.

Cookies

We might use 'cookies' to collect data to help us to manage our website and improve our online services. 'Cookies' are small files placed on your computer when you visit a website. 'Cookies' capture how often you visit pages and other data about browsing preferences. 'Cookies' are not used to identify people but can help us to provide a more personalised online experience. Users can configure their browsers to manage, accept or reject cookies.

Embedded videos

We use YouTube to host embedded videos on our website. When a video is played from our website, YouTube collects information about activity such as videos watched and interaction

with content and advertisements. We use this information to improve our website and its content. YouTube is hosted overseas.

Third party sites and platforms

We are not responsible for any acts or practices that take place on third party platforms and/or websites that might breach privacy, therefore we recommend that individuals always examine the terms and conditions and privacy policy of the relevant platform and/or website.

Applications and feedback

We collect information from people when they apply for one of our products or services, when they report maintenance, or when they provide feedback such as an appeal, complaint, or compliment. We use the information we collect to respond to maintenance reports and feedback and to assess applications for products and services. We use Jotform and Gravity Forms to collect this information. Jotform is hosted overseas, and Gravity Forms is hosted in Australia.

Social media

We use social media platforms to communicate with people about the work we do. We may collect personal information from people when they communicate with us using these platforms. The social media platform may also collect personal information of users for its own purposes. Social media platforms have their own privacy policies which are available on their websites.

Direct marketing

We may use personal information from time to time to send marketing materials to current or prospective customers. For example, we collect information that people provide to us when they sign up to a mailing list or register for events or updates. We use Campaign Monitor to manage mailing lists and registrations. Campaign Monitor collects data about which emails are opened, which links are clicked Campaign Monitor stores data in a US-based data centre and uses data processing locations in the US, Australia and Germany.

If individuals wish to cease receiving marketing information, please contact us directly on the contact details listed at the end of this Policy asking to be removed from our mailing lists or use the "unsubscribe" or "update your preferences" facilities included in all our marketing communications.

Recruitment

We will handle all personal information of job applicants in accordance with the APPs. If we are sent an application to be considered for an advertised position (or unsolicited), the personal information contained in the application may be used to assess suitability for employment with us. This personal information may be disclosed to our related bodies corporate and/or service providers for human resources management activities. As part of the application process, individuals may be asked for consent to the disclosure of personal information to those people nominated to provide references. A refusal to provide any of this information, or to consent to its proposed disclosure, may affect the success of the application.

Data breaches

A notifiable data breach scheme is currently in place in Australia. We are committed to adhering to this scheme as an important step in preventing and managing serious privacy breaches.

A "data breach" means unauthorised access to, or disclosure, alteration, loss, or destruction of, personal information—or an action that prevents us from accessing personal information on

either a temporary or permanent basis. An "eligible data breach", in accordance with the Privacy Act, occurs when there is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates and we are unable to prevent the likely risk of serious harm with remedial action.

We, including all our people, take breaches of privacy very seriously. If we suspect a privacy breach has occurred, our priority is to contain and assess the suspected breach in accordance with our Data Breach Response Plan. In doing so, we will:

- take any necessary immediate action to contain the breach and reduce the risk of harm;
- determine the cause and extent of the breach;
- consider the types of information involved, including whether the personal information is sensitive in nature;
- analyse the nature of the harm that may be caused to affected individuals;
- consider the person or body that has obtained or may obtain personal information as a result of the breach (if known); and
- determine whether the personal information is protected by a security measure.

If we believe an eligible data breach has occurred we will, as soon as practicable, notify the Commissioner and all affected individuals or, if it is not possible to notify affected individuals, provide public notice of the breach (in a manner that protects the identity of affected individuals).

Resolving privacy issues and further information

We are committed to working with people to resolve any issues or concerns about privacy.

Anyone who feels that they have been affected by a decision made under this policy has a right to appeal the decision.

Any issues, concerns, complaints, questions and appeals relating to privacy should be directed to our Privacy Officer.

Contacting our Privacy Officer

Phone: 1800 573 370

Email: privacyofficer@sgch.com.au

Mail: Privacy Officer
PO Box 348
Hurstville BC 1481

If a person receives our response to a complaint and is still unhappy, they have the option of referring their complaint to the Office of the Australian Information Commissioner (OAIC). If the complaint relates to health information, the person may also ask for a review from the Information and Privacy Commission NSW.

Recording conversations/meetings with us

When customers contact us at the Customer Care Hub, they will be advised that that initial call may be recorded for training and service improvement purposes.

We do not allow customers to record conversations and meetings with us. However, if requested, we may provide a written statement of agreed actions following a meeting or conversation.

Relevant legislation/legislative instruments

- *Privacy Act 1988* (Cth)
- *Health Records and Information Privacy Act 2002* (NSW)

Policy information

Version:	12
Approved:	November 2022
Reviewed:	November 2022
Review frequency:	24 months
Responsible team/position:	Privacy Officer