

Compliance: Privacy Policy

| | | | |
|---|----------------|--------------|-----------|
| Policy No. | C-3 | | |
| Version No. | 4 | Date: | June 2022 |
| Board meeting date of acceptance | June 2022 | | |
| Effective date | June 2022 | | |
| Review date | July 2024 | | |
| Related policies and documents | Probity Policy | | |

Scope

This policy applies to all staff, tenants, applicants, partner organisations and stakeholders involved with Amélie Housing.

Policy Statement

It is the policy of Amélie Housing to comply with the Australian Privacy Principles (APP-2014) in how we treat personal information collection, storage, and management. This includes:

- what information Amélie Housing can collect
- how Amélie Housing collects information (verbally, in writing, electronically)
- how Amélie Housing stores and protects personal and health information in shared access systems such as the NSW Housing Register and
- the purposes for which your personal information is collected, held, used, and disclosed
- how Amélie Housing can use and disclose your information, including special protection for health and other sensitive information
- how you can find out what information we hold and correct it if it is wrong
- how you can complain or enquire about breaches of your privacy
- whether Amélie Housing is likely to disclose your personal information to any overseas recipients or another party

This policy applies to all staff, tenants, applicants, partner organisations and stakeholders involved with St Vincent De Paul Amélie Housing.

Compliance

This policy assists Amélie Housing in complying with:

| Compliance Document | Section/Number | Area |
|--|----------------|-----------------------------|
| Evidence Guidelines National Regulatory Framework for Community Housing | 5b | Probity |
| | 4c | Governance |
| National Community Housing Standards | 3.5 | Privacy and confidentiality |

Privacy Policy

Collecting personal information

At Amélie Housing, we collect personal information from applicants, tenants, members of tenants' households, job applicants, staff, volunteers, and others, including contractors, visitors and others that engage with our organisation.

It is noted that employee records are not covered by the Australian Privacy Principles or the Health Privacy Principles, which relate to a current or former employment relations between our organisation and the employee.

What Kinds of Personal Information Do We Collect?

The kinds of personal information we collect is dependent upon whose information we are collecting and why we are collecting it; however, in general terms, we may collect:

- Personal information including names, addresses and other contact details; dates of birth; next of kin details; financial information, photographic images, and attendance records.
- Sensitive information (particularly concerning providing appropriate housing services and our work health and safety obligations) includes where relevant religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, family court orders and criminal records.
- Health Information (particularly about providing appropriate housing services and complying with our work health and safety obligations) including medical records, disabilities, individual health care plans, and counselling reports,

How do we collect your personal information?

How we collect personal information will depend on whose information we are collecting. If it is reasonable and practical to do so, we collect personal information directly from you. Where possible, we have attempted to standardise the collection of personal information by using specifically designed forms (e.g., an Application Form or a Health Information Disclosure Form). However, given the nature of our operations, we often also receive personal information by email, letters, and notes, over the telephone, in face-to-face meetings, through financial

transactions and surveillance activities such as using CCTV security cameras or email monitoring.

We may also collect personal information from other people (e.g., referring agencies, service providers including health service providers and partner agencies) or independent sources (e.g., a telephone directory); however, we will only do so where it is not reasonable and practical to collect the information from you directly.

How we use personal information

We only use personal information necessary for one or more of our functions or activities (the primary purpose) or for a secondary purpose that you would expect or to which you have consented.

Our primary uses of personal information include but are not limited to:

- providing housing, accommodation, and related services;
- satisfying our legal obligations, including our duty of care to tenants, workers, and child protection obligations;
- keeping tenants informed as to community housing matters through correspondence, newsletters, and magazines;
- marketing, promotional, and fundraising activities;
- helping us to improve our day-to-day operations, including training our staff; systems development; developing new programs and services; undertaking planning, research and statistical analysis using de-identified information wherever practicable;
- administration, including for insurance purposes;
- the employment of staff;
- the engagement of volunteers.

We only collect sensitive information necessary for one or more of these functions or activities. We also collect sensitive information if we have the person's consent or if it is necessary to lessen or prevent a serious threat to life, health or safety. Another permitted general situation would be locating a missing person or a legal health situation.

Storage and Security of Personal Information

We store personal information in various formats, including on databases, hard copy files and personal devices, including laptop computers, mobile phones, cameras and other recording devices.

The security of your personal information is important to us, and we take all reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification, or disclosure.

These steps include:

- Restricting access to information on our databases on a need-to-know basis with distinct levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff know they are not to reveal or share personal passwords.
- Ensuring that sensitive and health information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need-to-know basis.
- Implement physical security measures around the buildings and grounds to prevent break-ins.
- We are implementing computer security systems, policies, and procedures to protect personal information storage on our computer networks.
- Implementing human resources policies and procedures, such as email and internet usage, confidentiality, and document security policies, to ensure that staff follow correct protocols when handling personal information.
- They are undertaking due diligence concerning third-party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.
- We require third-party service providers to sign confidentiality and privacy undertakings where practicable.

Personal information we hold no longer needed is destroyed securely, deleted or de-identified as appropriate.

Our website may contain links to other websites. We do not share your personal information with those websites and are not responsible for their privacy practices. Please check their privacy policies.

When we disclose personal information

We only use personal information for the purposes it was given to us or for purposes related (or directly related in the case of sensitive information) to one or more of our functions or activities. We may disclose your personal information to government agencies, our service providers, agents, contractors, partner support agencies, business partners and other recipients from time to time, only if one or more of the following apply:

- you have consented;
- you would expect us to use or disclose your personal information in this way;
- we are authorised or required to do so by law;
- disclosure will lessen or prevent a serious threat to the life, health, or safety of an individual or to public safety;
- where another permitted general situation or permitted health situation exception applies;
- disclosure is necessary for a law enforcement-related activity.

Disclosure of personal information to overseas recipients

In certain circumstances, we may disclose personal information about an individual to overseas recipients, such as storing information with a "cloud service provider" that stores data outside Australia. We will take all reasonable steps not to disclose an individual's personal information to overseas recipients unless:

- We have the individual's consent (which may be implied); or
- We have satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principles or a similar privacy regime; or
- We form the opinion that the disclosure will lessen or prevent a serious threat to the life, health, or safety of an individual or public safety; or
- We are taking appropriate action about the suspected unlawful activity or serious misconduct

How we ensure the quality of your personal information

We take all reasonable steps to ensure the personal information we hold, use, and disclose accurate, complete, and up to date.

We maintain and update personal information when individuals advise us or when we become aware through other means that their personal information has changed. Please contact us if any of the details you have provided change. You should also contact us if you believe the information we have about you is inaccurate, complete, or up to date.

How to gain access to your personal information we hold

By contacting us, you may request access to the personal information we hold about you or request that we change the personal information.

If we do not agree to provide you with access or amend your personal information as requested, you will be notified in writing. Where appropriate, we will provide you with the reason/s for our decision. If the rejection relates to a request to change your personal information, you may make a statement about the requested change, and we will attach this to your record.

Privacy Complaints

If you wish to make a complaint about a breach by us of your privacy (that includes the Australian National Privacy Principles), you may provide your written complaint by email, letter, fax or by personal delivery to any one of our contact details as noted below. You may also make a complaint by phoning or face to face.

We will respond to your complaint within a reasonable time (usually no longer than 30 days), and we may seek further information from you to provide a complete response.

Your complaint may also be taken to the Office of the Australian Information Commissioner or the NSW Privacy Commissioner.


How to Contact Us

You can contact us about this policy or your personal information by:

- Emailing: contact@amelie.org.au
- Calling: 02 9568 0219
- Writing to our Privacy Officer at 2c West Street Lewisham NSW 2049

If practical, you can contact us anonymously (i.e., without identifying yourself) or using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

Changes to our privacy and information handling practices

This Privacy Policy is subject to change at any time. Please check our [website](#)  regularly for any changes.