GOVERNANCE: PRIVACY POLICY

POLICY STATEMENT

Haven Home Safe (HHS) is committed to upholding its obligations to protect the privacy of personal and sensitive information about its clients, staff, visitors, contractors, partners and others that come in contact with the organisation and will, to the extent reasonably possible, protect personal information of staff, clients and renters from unauthorised access and disclosure (need-to-know); unauthorised modification (integrity of the information); and inappropriate transmission, transportation, storage, disposal, and loss of information.*

Guiding Principles:

Haven is committed to abiding by the *Australian Privacy Principles* enshrined in the Privacy Act 1988 (Cth)* regarding:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Consent to the collection and/or disclosure of personal information
4. Collection of solicited personal information
5. Dealing with unsolicited personal information
6. Notification of the collection of personal information
7. Use or disclosure of personal information
8. Direct marketing
9. Cross-border disclosure of personal information
10. Adoption, use or disclosure of government related identifiers
11. Quality of personal information
12. Security of personal information
13. Access to personal information
14. Correction of personal information

Source:
https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference

Purpose

This Level 1 policy outlines the principles and processes used to protect the privacy rights of individuals and comply with relevant privacy and data protection legislation.

Scope

This Policy applies to all HHS Directors, staff, renters, clients, visitors, contractors, partners, and others that come into contact with the organisation.

Roles and Responsibilities

Details of roles and responsibilities are outlined in the *Privacy Standard Operating Procedure (SOP)*, Section 2 pg 3.

Details

HHS will promote a culture of privacy awareness where staff are trained and supported to protect the privacy of personal information and are aware of how to identify and report potential or actual privacy breaches and/or information security incidents. (Refer Attachments to SOP pp 8+)

Who we collect information from:

We collect personal information from or about applicants for housing vacancies, renters, members of renters' households, service support clients, employment candidates, staff, contractors who are individuals, visitors, and other individuals that come into contact with our organisation.

What information we collect: *(Refer also to SOP Section 3 pg 3)*

Subject to *why* we are collecting information and *who* we are collecting it from, we may collect personal and/or sensitive information, including health information, about individuals that is reasonably identifiable and necessary to collect.

How we collect, use and manage personal information about individuals.

We collect and use personal information with the consent of the individual or as permitted by law where it is reasonably necessary to do so for the provision of one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected and that has been disclosed.

When seeking consent from an individual to collect their personal information, HHS will be transparent and unambiguous about what information is being collected, why it is being collected, how it will be used, how long it will be retained, who it will be shared with or disclosed to, and how and when it will be disposed of.

At any time a person can withdraw their consent, object to the use of their information, request their information be deleted, request to access their information or seek an explanation of how their information is being used.

**NB: All references to 'personal information' should be taken to include personal or sensitive information or data.*

Recommended by: Executive	22 Mar 2023	**Endorsed by:** Board CQRC	28 Mar 2023
Scheduled review:	6 April 2024	**Policy level:** 1 **Version:** Final	**Risk Rating:** HIGH

This policy has been approved by Haven Home Safe's Board.

Signed: **Name/Position:** [Damien Tangey, Chair BoD] 6 April 2023

We collect information directly from the individual unless it is unreasonable or impracticable to do so, and only collect information that is reasonably required for the purpose of the activity for which the information has been collected or otherwise disclosed

Personal information can be collected in many forms from the individual, from digital sources including SMS/email/social media, or from other sources including CCTV security coverage of multi-occupancy residential properties and HHS offices.

(CCTV coverage will only be in place in communal or public spaces, and signage will be posted. CCTV footage will only be used internally by HHS or be released to Police in relation to the investigation of an incident, to manage a situation, or as otherwise required by law.)

HHS will ask the client or renter for general consent for disclosure of information before sharing their personal or sensitive information with anyone outside of the organisation such as referring agencies, Centrelink, Consumer Affairs, advocates etc., for the purpose of linking the client or renter to additional service supports or for any other disclosed purpose. (*Refer to SOP Section 3 pg 4 'Disclosure…').*

Consent may be obtained at any time prior to a disclosure, such as at the time a form or an application is completed.

A person has the right to decide not to share their identity; to use a pseudonym; to prevent access to some of their information; or to partially or entirely restrict access to their personal information when submitted as a written request, subject to any such request being lawful. However, this may affect HHS' ability to provide the best possible service and/or employment support.

HHS has a much higher standard of care in relation to the collection and sharing of information about children and vulnerable adults.

If HHS receives unsolicited personal information about a person, HHS will only hold, use and/or disclose if we could otherwise do so had we collected it by normal means. Otherwise, HHS will destroy, delete or de-identify the information as appropriate, noting that HHS also has an obligation to take reasonable steps to also protect de-identified or aggregated data/information. (*For further information refer* Privacy SOP *Section 3 pg. 3*)

Maintaining the Quality of Personal Information

It is important to us that Personal Information is up to date. We will take reasonable steps to make sure that Personal Information is accurate, complete, and up to date. If an individual finds that the information we have is not up to date or is inaccurate, we will update our records once notified to enable HHS to continue to provide quality services.

Disclosure of Personal Information

HHS must only disclose personal information for the purpose for which it was collected (e.g. to provide support services, tenancy services, or personnel-related matters), and with written consent, **UNLESS**:

- The individual to whom the information relates was informed when the information was collected that it might be disclosed in this way, or has provided prior informed consent
- HHS is lawfully required to do so
- Where disclosure will lessen or prevent a serious threat to the life, health, or safety of an individual or to public safety.

Personal or sensitive information will not be disclosed to overseas recipients except where there is a "Duty of Care" responsibility (see Exemptions for Disclosure).

HHS will take reasonable steps to ensure personal information is only shared with the consent of the person to whom it pertains and will amend records where a person requests a change or cancels their permission to share information as a written request. HHS will aggregate data or deidentify personal data for reporting purposes.

Exemptions for Disclosure

A legal requirement to disclose personal information may override the individual's right to confidentiality; this is known as a "Duty of Care" (refer to *Duty of Care Policy*). Situations where this may occur include the following:

- Where there is serious risk of abuse or physical harm to the individual or other person
- When the disclosure is necessary, appropriate, or otherwise required to be disclosed by law

- A concern for a child's safety or wellbeing (refer to *Child Safety and Wellbeing Policy*) or as part of the Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS).

Where disclosure of personal information meets the *Exemptions for Disclosure* criteria (above), such information **must not** be disclosed to a lawful entity (such as Victoria Police, the Courts, or legal representatives of any party), or a regulatory entity (such as a representative of a relevant government department (eg DFFH), Office of the Housing Regulator, Office of the Disability Services Commissioner, etc.), Ministers of the Crown or their staff, or the Office of the Information Privacy Commissioner without the prior endorsement of the Privacy Officer to either the Chief Operations Officer, Chief Business Services Officer, or CEO for approval. Any such approvals granted will be recorded. Disclosure will not be made to members of the public under any circumstances.

Storage and Security of Personal or Sensitive Information

HHS stores personal information in a variety of formats including cloud storage, databases, hard copy files and electronic devices including laptop computers, mobile phones, cameras, and other recording devices. HHS will take all reasonable steps to ensure personal information is protected from misuse, loss, unauthorised access, modification, or improper disclosure. Personal information will be retained for the period required by law in relation to the retention of data.

Accessing personal information

Individuals have the right to request access to their personal information and request that we change or update their personal information, by contacting us.

Generally (subject to Australian law), we will give individuals full access to their personal information within a reasonable time and in the manner requested . However, there may be some circumstances when this is not possible, including where:

- HHS no longer holds or uses the information
- providing access would have an impact on the privacy of others or the safety of staff
- the request is reasonably considered to be frivolous or vexatious
- providing access would be unlawful.

If HHS do not provide with a person with access to all their personal information, HHS will tell them the reason why HHS has not done so.

Privacy Complaints

Individuals who have a complaint in relation to privacy have a number of options:

1. Speak to HHS staff about their concerns , or make a complaint on HHS' website, in writing or in person. HHS will respond to the complainant within three business days to advise how HHS intends to resolve the issue. (Online:https://havenhomesafe.org.au/contact/feedback-complaints/ OR Email: feedback@hhs.org.au) OR Mail to Privacy Officer Haven; Home, Safe PO Box 212, Bendigo, VIC 3552 OR Call Phone: 1300 428 364

2. If a complainant is not happy with HHS' response, or wants to make a direct privacy complaint they can make a complaint to:

Victorian Privacy Commissioner
Email:enquiries@ovic.vic.gov.au
www.ovic.vic.gov.au

Office of the Housing Registrar
Tel:03 7005 8984
Email:housingregistrar@dtf.vic.gov.au
www.vic.gov.au/housing-registar

Australian Information Commissioner
Tel:1300 363 992
www.oaic.gov.au

Health Complaints Commissioner
Tel:1300 582 113
www.hcc.vic.gov.au

Relativities

For further information about the Australian Privacy Principles and the Health Privacy Principles visit Victorian Office of the Information Commissioner (OVIC) website: https://ovic.vic.gov.au/

For more details refer to *Privacy SOP*, Section 7.

This Policy replaces:

- Operations Privacy Policy

- Client Privacy Confidentiality Policy
- Privacy Data Security Policy

END

Australian Privacy Principles — a summary for APP entities

from 12 March 2014

Australian Government
Office of the
Australian Information Commissioner

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.