

## 4.60 Policy

## Privacy of Personal Information

Australian Nursing Home Foundation (ANHF) respects and maintains the privacy and security of the personal information of our staff, volunteers, applicants, residents, participants, tenants, donors, suppliers, job applicants, and visitors to ANHF sites/facilities. This includes sensitive information.

We comply with all privacy related laws, regulations and the Australian Privacy Principles (**APPs**). We will take all reasonable steps to protect the personal information we hold from misuse and loss, and from any unauthorized access, modification or disclosure.

Our summarised **Privacy Statement** is published on our website and readily available to our stakeholders.

### Record of policy development

Version	Date approved	Date for review
2026/Version 4.0	01/2026	2028 or earlier as needed

### Responsibilities and delegations

This policy applies to	Board, workers, volunteers, residents, participants, tenants, donors, suppliers, job applicants, and visitors
Specific responsibilities	Privacy Officer
Policy approval	CFO

### Policy context – this policy relates to:

Standards	<ul style="list-style-type: none"> <li>Strengthened Aged Care Quality Standards (2025)</li> </ul>
Legislations	<ul style="list-style-type: none"> <li><i>Aged Care Act 2024 (Cth)</i></li> <li><i>Aged Care Rules 2025 (Cth)</i></li> <li><i>Privacy Act 1988 (Cth)</i></li> <li><i>Privacy and Other Legislation Amendment Act 2024 (Cth)</i></li> <li><i>Privacy and Personal Information Protection Act 1998 (NSW)</i></li> <li><i>Health Record and Information Privacy Act 2002 (NSW)</i></li> </ul>
Related documents	<ul style="list-style-type: none"> <li>Office of the Australian Information Commissioner (<b>OAIC</b>) Australian Privacy Principles Guidelines (2025)</li> </ul>

## Definitions

TERM	DESCRIPTION
<b>APP entity</b>	App entity means an agency or organisation and has the meaning set out in s 6(1) of the <i>Privacy Act 1988 (Cth)</i> .
<b>APPs</b>	APPs means the Australian Privacy Principles which are set out in Schedule 1 of the <i>Privacy Act 1988 (Cth)</i> .
<b>Data Breach</b>	<p>A data breach happens when personal information (such as a person's name, contact details, medical records, or banking details) is:</p> <ul style="list-style-type: none"> <li>• accessed or released without proper authorisation, or</li> <li>• lost and likely to be accessed or released without authorisation.</li> </ul> <p>Examples of a data breach include when:</p> <ul style="list-style-type: none"> <li>• A USB or mobile phone that holds customers' personal information is stolen</li> <li>• A database containing personal information is hacked</li> <li>• Someone's personal information is sent to the wrong person.</li> </ul>
<b>Personal information</b>	Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.
<b>Sensitive information</b>	Information or an opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual orientation or practices; or criminal record that is also personal information. Also, information that is health information about an individual; genetic information about an individual that is not otherwise health information; biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or biometric templates.

<p><b>Health Information</b></p>	<p>“Health information” means:</p> <ul style="list-style-type: none"> <li>(a) <u>personal information</u> that is information or an opinion about: <ul style="list-style-type: none"> <li>(i) the physical or mental health or a disability (at any time) of an individual, or</li> <li>(ii) an individual’s express wishes about the future provision of <u>health services</u> to him or her, or</li> <li>(iii) a <u>health service</u> provided, or to be provided, to an individual, or</li> </ul> </li> <li>(b) other <u>personal information</u> collected to provide, or in providing, a <u>health service</u>, or</li> <li>(c) other <u>personal information</u> about an individual collected in connection with the donation, or intended donation, of an individual’s body parts, organs or body substances, or</li> <li>(d) other <u>personal information</u> that is <u>genetic information</u> about an individual arising from a <u>health service</u> provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a <u>genetic relative</u> of the individual, or</li> <li>(e) <u>healthcare identifiers</u></li> </ul>
----------------------------------	---

## 1. Collection of Personal Information

- ANHF will only collect personal information (including sensitive information) if it is reasonably necessary for our functions, services, or activities.
- In most cases, ANHF will only collect information directly from those who have given their consent. The person giving the consent has the right to correct personal information or withdraw the consent to share information at any time.
- Personal information may be gathered from official forms, telephone calls, faxes, emails, face to face meetings, interviews, job applications, surveys, and assessments.
- Where personal information (including sensitive information) is collected indirectly from publicly available sources or from third parties (e.g. other Government agencies, authorised representative), we will inform the individual that we hold his or her personal information.
- Unsolicited personal information and information that is no longer required for the delivery of health services will be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.
- The potential consequences of not allowing us to collect and hold the required personal information are that we may be unable to:
  - Provide appropriate quality health care and services and meet our legislated obligations
  - Meet the individual requirements of the resident, participant or tenant
  - Provide continuing employment to an employee
  - Continue with the services of a contractor or volunteer

## 2. Unsolicited Personal Information

If we receive “unsolicited information” such as personal information that is not relevant to the services or activities of ANHF, such information will be de-identified or destroyed as soon as practicable.

## 3. Sharing or Disclosure of Personal Information

- Personal information may be disclosed if we:
  - Are required or authorized by Australian law or a court / tribunal order
  - Reasonably believe that the disclosure is necessary to lessen or prevent a serious or imminent threat to an individual’s life, health or safety, or a serious threat to public health or safety
  - Have reason to believe that an unlawful activity has been, is being, or may be engaged in
- Personal information may be disclosed to other persons as part of the provision of health services, including:
  - Other health care professionals that are or may be involved in the care of residents/ participants/tenants or employees including general practitioners, hospitals, and other allied health providers
  - Other external agencies that we have contracts with to provide services to residents/participants and employees on our behalf. In circumstances where this is necessary, these external agencies are required to provide confirmation of their compliance with the *Privacy Act 1988 (Cth)*.
  - Funding bodies and other government agencies as required by Commonwealth and State legislations.
  - The person designated by the residents/participants as the “substitute decision maker” for giving and accessing their information.

- Personal information relating to residents/participants/tenants, workers will not be used for other purposes such as fundraising or direct marketing activities without seeking written consent of the person or the “substitute decision maker” for the residents/consumers/ tenants.

#### **4. Disclosure of Personal Information Overseas**

- ANHF does not routinely disclose personal information overseas.
- If it is likely to disclose personal information to overseas recipients, ANHF will comply with this Policy and take reasonable steps to ensure that we do not breach the APPs in relation to that information.
- ANHF does use social media platforms (e.g. Facebook, Whatsapp, Wechat) to post about its services, employment opportunities, and events. Should an individual choose to interact with ANHF through any of these platforms, it is the individual’s responsibility to review and accept the privacy policy of that platform before interacting with ANHF.

#### **5. Security of Personal Information**

- ANHF will take all reasonable steps to protect the personal information we hold from misuse and loss, and from unauthorized access, modification or disclosure.
- All of our electronic systems that hold personal information have up to date security protection systems. These are reviewed on a regular basis and tested to ensure they are updated and effective.
- We will train all staff with access to personal information about their obligations concerning confidentiality and security of personal information.
- When no longer required, personal information will be destroyed or archived securely following recognised security and storage processes.
- In the event of loss of personal information, we will:
  - Seek to identify and secure the breach to prevent further breaches
  - Assess the nature and severity of the breach
  - Commence an internal investigation in relation to the breach
  - Report the breach to police where criminal activity is suspected
  - Notify the OAIC if appropriate
  - Inform the affected individual(s) where appropriate

#### **6. Access to Personal Information**

- We will take all reasonable steps to provide access to the personal information that we hold within a reasonable period of time in accordance with the Australian Privacy Principles.
- Requests for access to the personal information we hold should be made in writing to the Privacy Officer.
- We may not provide access to the personal information we hold about an individual when:
  - Release of the personal information would be unlawful
  - The information may be subject to legal proceedings
  - Release of the personal information would pose a serious threat to the life, health or safety of an individual or to public health or public safety
  - Release is likely having an unreasonable impact upon the privacy of other individuals
  - The information could compromise our business operations
  - The request is assessed as vexatious or frivolous
- We will provide reasons for denying or refusing access to personal information in writing. This correspondence will include information concerning the mechanisms for lodging a complaint.

## **7. Quality and Correction of Personal Information**

- We will take all reasonable steps to ensure that the personal information we collect, use, hold, or disclose is accurate, complete and up to date.
- Individuals may request, in writing, that personal information we hold is corrected if it is inaccurate, out of date, incomplete, irrelevant or misleading.
- We will take all reasonable steps to correct the personal information we hold.
- If appropriate, we will provide reasons for not complying with requests to correct personal information in writing.

## **8. Use of Government Issued Identifiers**

We will not use government issued identifiers (e.g. Medicare number, driver's licence number) as its own identifier of individuals.

## **9. Anonymity**

We will provide individuals with the option of not identifying themselves, or of using a pseudonym where it is lawful and reasonably possible to do so.

## **10. Disposal of archived documents**

Confidential or sensitive materials must be destroyed securely through shredding, incineration, or other approved methods to prevent unauthorized access or misuse. Records of document disposal, including dates and methods used, should be maintained for accountability and audit purposes. Employees involved in the process must adhere to the organization's confidentiality and data protection policies.

## **11. Breaches of Privacy**

Where a person suspects or believe that a breach of privacy has occurred, he or she should inform or report the incident/concern in writing to the Privacy Officer. All privacy breaches will be dealt with confidentially and promptly.

## **12. Notifiable Data Breaches Scheme**

The Privacy Officer is required to notify the OAIC and all affected individuals where a data breach is likely to result in serious harm to an individual whose personal information is involved.

The Privacy Officer will also notify the company's Insurer immediately and obtain professional advice under the appropriate insurance policy.



### 13. Complaints

Anyone can make a complaint about the way ANHF deal with privacy issues by contacting the Privacy Officer as soon as possible. ANHF will respond to the complaint with 30 days and may seek further information in order to provide a full and complete response.

To facilitate prompt response, please assist by ensuring that you:

- Identify yourself, if appropriate.
- Give a brief description of why you think that your personal information was compromised.
- Advise how you would like ANHF to resolve the matter.

If the complainant is not satisfied with ANHF's response, he or she may refer the complaint to the OAIC via their website.

### 14. Contacts

#### **ANHF Privacy Officer's contact details:**

By email to: [PrivacyOfficer@anhf.org.au](mailto:PrivacyOfficer@anhf.org.au); or

By phone at: (02) 8741 0218 and asking to speak or leave a message for the Privacy Officer

#### **Office of the Australian Information Commissioner (OAIC) website:**

[www.oaic.gov.au](http://www.oaic.gov.au)