

THE NATIONAL TRUST *of* AUSTRALIA (NEW SOUTH WALES)

Privacy Management Plan



August 2026



1.	Executive Summary	4
2.	Introduction	5
2.1.	<i>Why do we have a Privacy Management Plan?</i>	<i>5</i>
2.2.	<i>What this Plan covers</i>	<i>5</i>
2.3.	<i>Responsibilities of staff and others</i>	<i>5</i>
2.4.	<i>Review of the Privacy Management Plan</i>	<i>5</i>
3.	Definitions and interpretations	6
4.	About us	6
4.1.	<i>Our functions</i>	<i>7</i>
4.2.	<i>Our stakeholders.....</i>	<i>7</i>
5.	Compliance	7
5.1.	<i>Personal Information</i>	<i>8</i>
5.2.	<i>Medical Health Information.....</i>	<i>8</i>
5.3.	<i>Exemptions to the Privacy Principles.....</i>	<i>8</i>
5.4.	<i>Other laws and guidelines that affect how we comply with the IPPs and HPPs</i>	<i>8</i>
6.	Collection	9
6.1.	<i>Types of information collected.....</i>	<i>9</i>
6.2.	<i>We collect personal information from individuals directly</i>	<i>10</i>
6.3.	<i>Storage of Personal Information.....</i>	<i>11</i>
6.4.	<i>Access of Personal Information</i>	<i>11</i>
6.5.	<i>Use of Personal Information</i>	<i>12</i>
6.6.	<i>Disclosure of Personal Information</i>	<i>12</i>
6.7.	<i>Sensitive Personal Information</i>	<i>12</i>
6.8.	<i>Public Registers.....</i>	<i>13</i>
6.9.	<i>Privacy Codes of Practice.....</i>	<i>13</i>
6.10.	<i>Public Interest Directions</i>	<i>13</i>
7.	Policies and Procedures	13
8.	Mandatory Notification of Data Breach Scheme	13
9.	Review rights and complaints	13
9.1.	<i>Internal review by the Trust.....</i>	<i>13</i>
9.2.	<i>Internal review process</i>	<i>14</i>
9.3.	<i>The NSW Privacy Commissioner's role in internal reviews</i>	<i>14</i>
9.4.	<i>External review by the NSW Civil and Administrative Tribunal.....</i>	<i>15</i>



9.5.	<i>Other ways to resolve privacy concerns</i>	15
10.	Promoting the Privacy Management Plan	15
10.1.	<i>Board and Governance</i>	15
10.2.	<i>Trust staff and volunteers</i>	16
10.3.	<i>Public awareness</i>	16
10.4.	<i>Contacting us.....</i>	16



1. Executive Summary

- This Privacy Management Plan outlines the National Trust of Australia (NSW)'s commitment to protecting the personal and health information we hold about our members, donors, staff, volunteers and event attendees.
- The Plan outlines how we comply with the legislation that governs the management of personal and health information including its collection, storage, access and use.
- The Trust is obligated to use personal information only for the purpose it was collected and must take reasonable steps to ensure that the information is used for its intended purpose, is relevant, accurate, up-to-date, complete and not misleading.
- Individuals with queries in relation to the National Trust's privacy obligations and/or their individual information are encouraged to contact the Trust's Privacy Officer privacy@nationaltrust.com.au.
- An individual can make a formal request to access or amend their personal information in a written submission outlined in section 5.4 of this document and by using the [Access or Amend Personal Information Form](#).
- An individual can apply for formal access to Government information under the [Government Information \(Public Access\) Act 2009 \(GIPA Act\) \(NSW\)](#).
- If an individual is unsatisfied in the way their privacy matters have been handled, we strongly encourage resolving the issue directly with the Trust, by contacting the Privacy Officer privacy@nationaltrust.com.au. If the matter is not resolved to the satisfaction of the individual, they have the right to request an internal review which is discussed in section 8.2. The form is available [here](#). The National Trust is committed to transparency and ensuring that our staff and volunteers are aware of and understand this Plan, particularly how it applies to their work. The Plan is publicly available on our [website](#) and is included when onboarding new staff and volunteers to the organisation.



2. Introduction

The National Trust of Australia (NSW) (Trust or Trust's) recognises the importance of safeguarding the privacy of individuals and is committed to complying with the [Privacy and Personal Information Protection Act 1998](#) (PIIP Act) and the Health Records and Information Privacy Act 2002 (HRIP Act). This Privacy Management Plan outlines our commitment to protecting the personal and health information we hold.

2.1. Why do we have a Privacy Management Plan?

We have a Privacy Management Plan because it is important for our members, donors, staff, volunteers and event attendees to understand how we handle their personal information. It is also a legal requirement under the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW).

This Plan outlines how we comply with the legislation that governs the management of personal and health information. It provides information on who to contact in case of any queries regarding their information, how to access or modify it, and what actions they should take if they suspect any potential breaches of these regulations.

We use this Plan to train our staff and volunteers on how to handle personal and health information properly. This helps us ensure we are following the laws correctly.

2.2. What this Plan covers

Section 33(2) of the PIIP Act sets out what is required to be covered in this Plan, namely:

- information about how we develop policies and practices in line with the PIIP Act and the HRIP Act
- the way we train our staff in these policies and principles
- our internal review processes and
- any other matters we think are relevant to the Plan regarding privacy and the personal and health information held by the National Trust.

2.3. Responsibilities of staff and others

All Trust employees and anyone working for the Trust, including volunteers, must follow the PIIP Act and HRIP Act. This also applies to the people working for organisations the Trust engages to provide services.

Trust staff and volunteers uncertain about how to comply with privacy obligations should seek advice from the Trust's Privacy Officer. Under section 62 of the PIIP Act:

It is a criminal offence, with a maximum penalty of 100 penalty units or imprisonment for 2 years, or both, for any employee (or former employee) of the Trust to intentionally use or disclose any personal information about another person, to which the employee has or had access in the exercise of his or her official functions, except as necessary for the lawful exercise of his or her functions.

2.4. Review of the Privacy Management Plan

We will review this Plan annually. We will review the Plan earlier if any legislative, administrative or systemic changes affect how we need to manage personal and medical health information.



3. Definitions and interpretations

For the purposes of this document and unless the context otherwise requires:

HPPs means the [15 health privacy principles](#) in the HRIP Act.

HRIP Act means the [Health Records and Information Privacy Act 2002 \(NSW\)](#).

IPPs means the [12 information protection principles](#) in the PPIP Act.

Medical health information means information about an individual's health or capacity to do any activity.
(The obligation regarding the collection and storage of this information comes with serious protection requirements).

Personal information means information or an opinion (including information or an opinion forming part of a database and whether it is recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

There are some kinds of information that are not personal information, e.g. information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment. Medical health information is generally excluded here as it is covered by the HRIP Act.

PO means the Privacy Officer for the Trust.

PPIP Act means the [Privacy and Personal Information Protection Act 1998 \(NSW\)](#).

Privacy is not defined in the law but is sometimes described as "the right to a sense of personal freedom, the right to have information about oneself used fairly, and a right to be left alone".

Privacy obligations means the "privacy principles" and any exemptions to those principles.

Privacy principles include the [12 IPPs](#), the [15 HPPs](#), and the public register rules.

Public register means a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee).

Sensitive personal information includes information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

Staff in the context of this Plan includes employees of the Trust, members, consultants, contractors (labour hire), and volunteers.

The Plan means the Privacy Management Plan of the National Trust of Australia (New South Wales).

4. About us

The National Trust of Australia (NSW) is a community-based, non-government organisation, committed to promoting and conserving New South Wales' natural, built and cultural heritage.

Established in 1945 by Annie Wyatt, the National Trust began with a mission to conserve Sydney's bushland and heritage architecture.



The National Trust (NSW) is Australia's leading heritage conservation charity. The Trust cares for magnificent gardens, galleries and house museums across New South Wales, while also leading the field in bushland management. Our advocacy efforts raise awareness for natural and built heritage under threat.

The Trust's vision is to bring the heritage of New South Wales to life now and into the future. This is made possible with the ongoing support of financial members, volunteers, donors and staff.

The National Trust (NSW) operates within the [National Trust of Australia \(New South Wales\) Act](#) and the [National Trust of Australia \(New South Wales\) Rules](#).

4.1. Our functions

The National Trust (NSW)'s core functions are to:

- Advocate for the conservation of built, cultural and natural heritage by engaging strategically with governments, industry, media and community.
- Identify, conserve and sustain our built, cultural and natural heritage by example, advice and support.
- Engage and educate our diverse communities through inclusive programs and stories that bring our collective histories to life for all generations.
- Maintain a comprehensive heritage register of landscapes, buildings, townscape, cemeteries and other culturally significant items worthy of conservation in New South Wales.
- Care for and act as a custodian for a collection of heritage places and items.
- Manage archives of rare photographs, maps, letters, sound recordings and other precious items.
- Regenerate bushland through conservation and biodiversity management services.
- Carry out philanthropy and fundraising for critical conservation projects.
- Manage tax deductible appeals to support conservation projects for churches, cemeteries, clubs and monuments.

4.2. Our stakeholders

We may collect personal information from the following stakeholders to carry out our functions and provide services:

- members
- donors
- volunteers
- visitors to our properties and galleries
- Trust employees
- private sector companies
- other cultural institutions.

5. Compliance

At the Trust, we are committed to protecting the privacy of our staff and stakeholders. We follow the PPIP Act and HRIP Act, which outline how we handle personal and medical health information.

We collect, store, use, and share various types of personal and medical health information as needed to perform our duties.



5.1. Personal Information

The PPIP Act applies to all personal information, except for health-related data, and mandates that all agencies comply with 12 information protection principles (IPPs). These IPPs cover the entire life cycle of information, including its collection, storage, usage and disposal. They also include provisions for data security, data accuracy, and the right to access and amend personal information. The Act also regulates personal information collection, use and disclosure. Personal information is any information or opinion that relates to a person who can be identified from the information.

There are specific exemptions that apply to the definition of personal information and health information held in the Trust's collections:

- Information about an individual that is contained in a publicly available publication.
- Information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

5.2. Medical Health Information

Medical health information is a specific type of personal information that contains information or opinions about an individual's physical or mental health or disability. It often comprises more private and comprehensive details about an individual that cannot be found in any other record, and any inappropriate use or disclosure of health information can have severe consequences.

As per the HRIP Act, medical health information is governed by 15 Health Privacy Principles (HPPs). It encompasses information about a person's disability as well as health and disability services provided to them. The Trust must adhere to the 15 HPPs to comply with the Act. These principles cover the entire information 'life cycle' and include rules related to anonymity, using unique identifiers, and sharing electronic health records.

5.3. Exemptions to the Privacy Principles

Exemptions to the privacy principles can be found in:

- the text of the PPIP Act
- the text of the HRIP Act
- regulations made under either Act
- Privacy Codes of Practice made by the Attorney General under the PPIP Act
- Privacy Codes of Practice made by the Minister for Health under the HRIP Act
- Public Interest Directions made by the NSW Privacy Commissioner under either Act.

5.4. Other laws and guidelines that affect how we comply with the IPPs and HPPs

This section contains information about the main laws that affect how we comply with the IPPs and HPPs.

5.4.1. Crimes Act 1900 (NSW)

Under this law, we must not access or interfere with data in computers or other electronic devices unless authorised.

5.4.2. Government Information (Public Access) Act 2009 (GIPA Act) and Government Information (Public Access) Regulation 2009 (NSW)

Under this law, individuals have the right to request access to government-held information, which may include personal or health information. In situations where an individual has requested access to someone else's personal or health information, we are required to consult with any affected third parties. Under the



[NSW GIPA Act](#), if it is decided that a third party's personal information should be released, we cannot share it until the third party has the opportunity to request a review of our decision.

5.4.3. The Mandatory Notification of Data Breach (MNDB) Scheme

The PPIP Act requires agencies to provide notifications to affected individuals in the event of an eligible data breach of their personal or health information by a NSW public sector agency or state-owned corporation subject to the PPIP Act.

5.4.4. Independent Commission Against Corruption Act 1988 (NSW)

Under this law, we must not misuse any information we have obtained while doing our jobs.

5.4.5. Public Interest Disclosures Act 1994 (PID Act) (NSW)

Under the PID Act, people working within a NSW public sector agency can make a public interest disclosure (PID) to the Information Commissioner about a failure to properly fulfil functions under the GIPA Act. We note that the definition of personal information under the PPIP Act excludes information contained in a public interest disclosure. This means that “personal information” received or collected under the PID Act is not subject to the IPPs or HPPs.

6. Collection

We only collect personal information for legal and purposes related to the performance of the Trust's operations.

6.1. Types of information collected

The Trust may collect the following types of personal for staff:

• addresses	• education	• phone number
• allowances (salary)	• email address	• previous employment
• bank account details	• health assessment	• private health insurance details
• citizenship	• membership number	• probation reviews
• country of birth	• marital status	• signature
• credit card details	• medical certificates	• skills assessment
• cv/resume	• full name	• superannuation details
• date of birth	• occupation	• tax file number
• deductions (salary)	• passport number	• third party information e.g. details of referees
• disability	• performance agreements	• next of kin
• driver's licence number	• performance development reviews	• workplace and safety constraints



The Trust may collect the following types of personal information for volunteers, members and event attendees:

• addresses	• email address	• phone number
• areas of interest	• full name	• postal address
• credit card details	• marital status	• signature
• date of birth	• membership number	

The Trust collects visitors' personal information during the delivery of services and programs, for example:

• appreciations and complaints	• philanthropic programs
• attendance lists for Trust functions and events	• advocacy/conservation/collections enquiries
• research and information requests	• website feedback
• Volunteer expressions of interest, enrolment	

The Trust does not collect Health Information of members, volunteers and visitors. The Trust collects other personal information about its employees, contractors, and volunteers for example:

• Health, workers compensation and rehabilitation information	• Personnel information (including contract information, child protection)
• Industrial, legal, grievance and disciplinary matters	• Recruitment records
• Learning and development records	• Banking details
• Leave and payroll data	

6.2. We collect personal information from individuals directly

The Trust collects personal information via telephone, email, correspondence, in-person, in hard copy and electronic forms.

As a general practice, we obtain personal information directly from the individuals concerned unless explicit authorisation has been granted to collect information through a third party. In cases involving individuals under the age of 16, personal information may be provided by a parent or guardian.

At the Trust, we are transparent about how we handle personal information. We inform people about why we collect their data and how they can access and update it. We respect privacy and provide clear information for informed choices about sharing their personal information.

When we gather personal information, we take reasonable steps to ensure that the person providing the information is aware of the following:

- the fact that we are collecting their information
- the specific purposes for which we are collecting their information
- who the intended recipients of their information are
- whether providing this information is a legal requirement or voluntary, and the potential consequences of not providing it, and
- their right to access and correct their information.



To communicate these points effectively, the Trust provides a privacy notice on forms when we request personal information and in our Web Privacy Statement.

We ensure that the personal information collected is relevant, accurate, is not excessive and does not intrude to an unreasonable extent on the individual's personal affairs.

The Trust will request only the personal information required to deliver services and fulfil its functions. When deciding what personal information to request, Trust staff will make sure it is no more than what is directly required and necessary for the specific function or purpose for which it is being gathered.

It's important to highlight that according to Section 4 of the PPIP Act, personal information is not considered as collected by a public sector agency if the agency receives it unsolicited.

6.3. Storage of Personal Information

We will store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure.

The Trust stores personal information directly in both digital and hard copy formats. Storage locations include both on-site and cloud-based databases and information storage services, email accounts, and hard copies retained in physical files.

Our commitment to safeguarding personal information is a high priority, and we have put in place protective measures to prevent unauthorised access, use, or disclosure. These measures include password protection using multi-factor authentication, single sign-on, access controls and audit logs for databases, secure filing cabinets, and restricted access to secure storage locations.

We ensure that all personal information is deleted from our systems or securely destroyed using designated secure disposal bins when it is no longer needed for the original purpose for which it was collected.

6.4. Access of Personal Information

We are transparent about the personal information we store about people, why we use the information and about their right to access and amend it.

The Trust will take reasonable steps to allow a person to ascertain whether we hold their personal information, the nature of the information, the main purpose for which the information is used, and the person's entitlement to gain access to the information.

Trust staff should also direct people to this Privacy Management Plan which is available on our [website](#).

We allow people to access their personal information without unreasonable delay or expense and update, correct or amend their personal information where necessary.

A person can also make a formal application to access or amend their personal information by submitting a written request by letter or email or by completing the [Access or Amend Personal Information form](#) stating the following:

- name and contact details
- state whether the application is being made under the PPIP Act or HRIP Act
- what personal information they want to access and/or amend
- the reason their personal information should be amended.

The Trust aims to acknowledge a request to provide access to or amendment of their personal information within 5 working days and aims to provide a response within 20 working days.



Government Information (Public Access) Act 2009 (GIPA Act) (NSW)

A person can also apply to access their personal information under the Government Information (Public Access) Act 2009 (GIPA Act) (NSW) by completing the [GIPA Access Application form](#).

The Trust is usually restricted from giving people access to someone else's personal or health information. The PPIP Act and HRIP Act give people the right to access their own information; they generally do not give people the right to access someone else's information. See section 6.6 below for exemptions to this restriction. The GIPA Act also includes an exemption to this rule as well.

6.5. Use of Personal Information

We only use personal information for the purpose it was collected, including secondary-related purposes such as program evaluation and customer satisfaction surveys.

The Trust will only use information for the purpose for which it was collected unless:

- the individual to whom the information relates has consented to the use of the information for that purpose or
- the other purpose for which the information is used is directly related to the purpose for which the information was collected or
- the use of the information for that other purpose is necessary to prevent or lessen a serious or imminent threat to the life or health of the individual to whom the information relates or of another person.

The Trust is obligated to use personal information only for the purpose it was collected. This means they must take reasonable steps to ensure that the information is used for its intended purpose, is relevant, accurate, up-to-date, complete and not misleading.

6.6. Disclosure of Personal Information

We will not disclose personal information to a third party unless the disclosure is directly related to the purpose for which it was collected, and we have no reason to believe the individual would object to the disclosure.

The Trust will not disclose personal information unless the individual concerned is reasonably likely to have been aware or has been made aware that information of that kind is usually disclosed to that other person or body. For example, applications to a particular award may be forwarded to the judges of the award.

The Trust may disclose personal information in instances where another Act or law authorises or requires us to do so. For example, to investigate an alleged breach of copyright under the Copyright Act 1968 (Cth).

Under section 26 of the PPIP Act a person can provide consent to disclose their personal information to someone that would not normally have access to it.

Under section 7 and section 8 of the HRIP Act an 'authorised person' can act on behalf of someone else. The HPPs also contain information about other reasons we may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual, to find a missing person or for compassionate reasons.

6.7. Sensitive Personal Information

We do not disclose sensitive personal information, that is, an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities without the individual's consent.

The Trust will not collect sensitive information however, if it does it will not disclose sensitive personal information without consent unless the disclosure is necessary to prevent a serious and imminent threat to



the life or health of the individual concerned or another person or where another Act or law authorises or requires us to do so.

6.8. Public Registers

A public register is a register of personal information that is required by law to be made publicly available or open to the public for inspection. The National Trust does not have any public registers.

6.9. Privacy Codes of Practice

A Privacy Code of Practice is a legal instrument made under Part 3 of the PPIP Act, which allows an agency to modify a privacy provision Information Protection Principle (IPP) or a public register provision or specify how that provision will apply in a particular circumstance. The Trust does not currently have a Privacy Code of Practice.

6.10. Public Interest Directions

A Public Interest Direction adjusts how the Information Privacy Principles (IPPs), or the Code of Practice applies to specific projects or activities undertaken by one or more public sector agencies. It's important to note that this direction does not authorise any behaviour that would be illegal otherwise, such as confidentiality requirements. There are no Public Interest Directions currently affecting the Trust.

7. Policies and Procedures

Trust staff should consult with the Privacy Officer when developing policies or procedures or amending them in a way that could change how we manage personal and/or medical health information.

The Privacy Officer will provide advice to ensure new and amended policies and procedures comply with the PPIP Act, HRIP Act and the Trust's Privacy Management Plan.

Trust policies and procedures that apply to Trust members and visitors are available on our [website](#).

8. Mandatory Notification of Data Breach Scheme

Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) establishes a rule called the NSW Mandatory Notification of Data Breach (MNDB) Scheme. This scheme makes it mandatory for all government agencies in NSW that follow the PPIP Act to inform the Privacy Commissioner and the people affected when certain data breaches occur.

The Mandatory Notification of Data Breach (MNDB) Scheme came into effect on 28 November 2023.

9. Review rights and complaints

9.1. Internal review by the Trust

People have the right to seek an internal review under the PPIP Act if they think we have breached the PPIP Act or HRIP Act relating to their own personal or health information. People cannot seek an internal review for a breach of someone else's privacy unless they are an authorised representative of the other person.

Under section 53(3) of the PPIP Act, an application for an internal review must:

- be in writing, and
- be addressed to the Trust, and
- specify an address in Australia to which a notice of the outcome of the review may be sent, and



- be lodged at the Trust offices within six months from the time the applicant first became aware of the conduct they want reviewed. We may also consider a late application for review.

If the complaint is about an alleged breach of the IPPs and/or HPPs, the internal review will be conducted by the Privacy Officer who:

- was not involved in the conduct, which is the subject of the complaint, and
- is an employee or an officer of the agency, and
- is qualified to deal with the subject matter of the complaint.

9.2. Internal review process

A person can apply for an internal review by completing our [Privacy complaint – request an internal review form](#) and sending it to the Privacy Officer by email, post or lodging the form in person. In most cases, the Privacy Officer will conduct the internal review. However, if the review pertains to the conduct of the Privacy Officer, an alternative reviewer will be appointed. The comprehensive review process is outlined in the [Complaints handling process](#).

The Trust aims to:

- acknowledge receipt of an internal review within 5 working days
- send a letter to the NSW Privacy Commissioner with details of the application. A photocopy of the written complaint will be provided to the NSW Privacy Commissioner
- complete an internal review within 60 calendar days.

The Privacy Officer will inform the applicant of the progress of the internal review, particularly if it is likely to take longer than first expected.

The Privacy Officer will respond to the applicant in writing within 14 calendar days upon deciding the outcome of the internal review as required under section 58(8) of the PPIP Act.

The response will include:

- the findings of the review (and the reasons for those findings), and
- the action we propose to take (and the reasons for taking that action), and
- the applicant's entitlements to have the findings and our proposed action reviewed by the NSW Civil and Administrative Tribunal (NCAT).

We will also send a copy of our response to the NSW Privacy Commissioner.

Statistical information about the number of internal reviews conducted will be included in the Annual Report of the National Trust of Australia (NSW) as required under the Annual Reports (Statutory Bodies) Act 1984 (NSW).

9.3. The NSW Privacy Commissioner's role in internal reviews

The Trust is required to notify the NSW Privacy Commissioner when an internal review request is received and of the proposed outcome. The NSW Privacy Commissioner is entitled to make submissions to the Trust outlining their view on the matter.

A person can also make a complaint directly to the NSW Privacy Commissioner if they think the Trust has breached the PPIP Act or HRIP Act relating to their own personal or health information.



Information and Privacy Commission

Level 17, 201 Elizabeth St
Sydney NSW

GPO Box 7011
Sydney NSW 2000
Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au

9.4. External review by the NSW Civil and Administrative Tribunal

If you are not satisfied with the result of an internal review we have undertaken, or if you do not receive a result within 60 days, you have the option to seek an external review by the NSW Civil and Administrative Tribunal (NCAT). You have 28 days after receiving the internal review decision to do so.

NCAT has the authority to make final decisions in an external review.

NSW Civil and Administrative Tribunal

Level 10. John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000 Phone: 1300 006 228

Website: www.ncat.nsw.gov.au

9.5. Other ways to resolve privacy concerns

We strongly encourage individuals to attempt an informal resolution of privacy matters with us before initiating the formal review process. It is advisable that individuals contact the Trust's Privacy Officer to discuss the issue prior to formalising a request for an internal review.

The Privacy Contact Officer:

- responds to enquiries about how we manage personal and medical health information
- responds to requests for access to and amendment of personal or medical health information
- provides guidance on broad privacy issues and compliance
- conducts internal reviews about possible breaches of the PPIP Act and HRIP Act (unless the subject of the review is the conduct of the Privacy Officer).

10. Promoting the Privacy Management Plan

10.1. Board and Governance

Our Board is committed to transparency about how we comply with the PPIP Act and HRIP Act, and we do this by:

- endorsing the plan and making it publicly available
- providing a copy of the Plan to relevant oversight bodies such as the Finance Audit and Risk Management Committee
- reporting on privacy issues in our annual report as required under the Annual Reports (Statutory Bodies) Act 1984 (NSW)
- attesting to complying with privacy legislation annually
- identifying privacy issues when implementing new systems or activities.



10.2. Trust staff and volunteers

We ensure that our staff and volunteers are aware of and understand this Plan, particularly how it applies to their work. Privacy breaches are more likely to occur when a Plan is not sufficiently relevant to the work that is done in the Trust. With this in mind, we have written this Plan and provided Procedures to staff and volunteers in a practical way so they can understand what their privacy obligations are, how to manage personal and medical health information in their work and what to do if unsure.

We make our staff aware of their privacy obligations by:

- publishing the Plan on our website
- including the Plan and Procedures in staff and volunteer induction packs
- providing advice on privacy issues that arise in day-to-day work.

When our staff and volunteers have questions about how to manage personal and medical health information and this Plan or associated procedures and guidelines, please refer them directly to your manager or the Privacy Officer.

10.3. Public awareness

This Plan is an assurance to our stakeholders of how we manage personal and medical health information. We will promote public awareness of this Plan by:

- writing the Plan in plain English
- publishing the Plan on our website in accordance with the open access provisions of the GIPA Act
- providing hard copies of the Plan free of charge on request
- tell people about the Plan when we answer questions about how we manage personal and medical health information.

10.4. Contacting us

Privacy Officer

National Trust Australia (New south Wales)

(02) 9258 0171

Email: privacy@nationaltrust.com.au

Website: www.nationaltrust.org.au/nsw/

Approved: Debbie Mills CEO and Executive Director	
Date of Approval:	12 August 2026

Responsibility for Review: Privacy Officer

Review Cycle: Annually

Next Review Date:	Reviewed:	Signed:
August 2027	/...../.....	
...../...../.....	/...../.....	