

# Privacy Management Plan and Guidelines (PMP)

---

TIPP 5.19

17 November 2023

## Acknowledgement of Country

We acknowledge that Aboriginal and Torres Strait Islander peoples are the First Peoples and Traditional Custodians of Australia, and the oldest continuing culture in human history.

We pay respect to Elders past and present and commit to respecting the lands we walk on, and the communities we walk with.

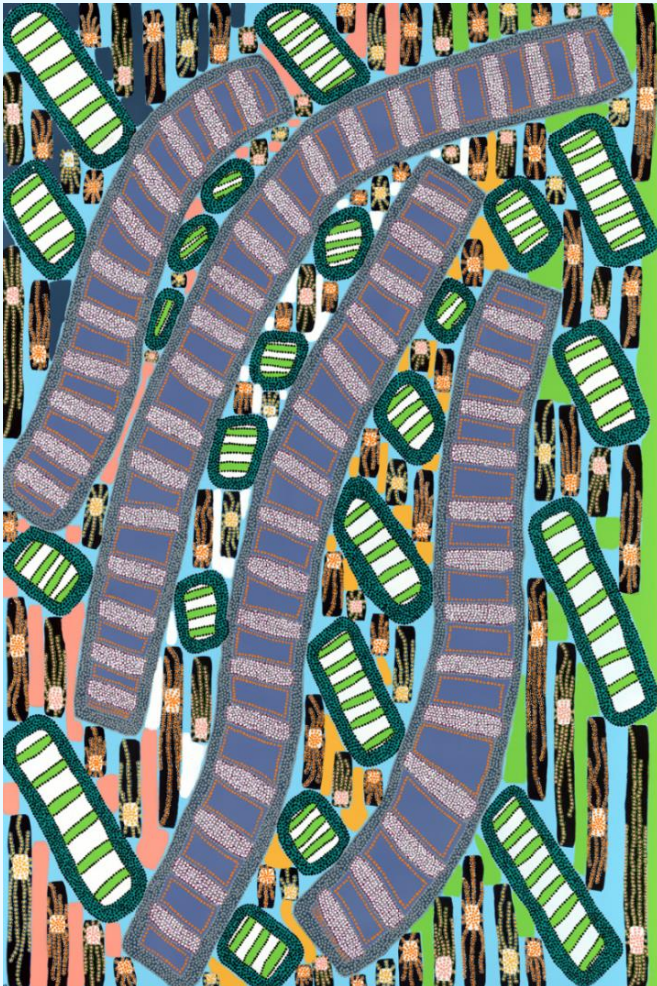
We celebrate the deep and enduring connection of Aboriginal and Torres Strait Islander peoples to Country and acknowledge their continuing custodianship of the land, seas and sky.

We acknowledge the ongoing stewardship of Aboriginal and Torres Strait Islander peoples, and the important contribution they make to our communities and economies.

We reflect on the continuing impact of government policies and practices, and recognise our responsibility to work together with and for Aboriginal and Torres Strait Islander peoples, families and communities, towards improved economic, social and cultural outcomes.

Artwork:

*Regeneration* by Josie Rose



Version	
Document number TIPP 5.19	Version number: 1
Original issue date	17 November 2023
To be reviewed on	19 February 2024

Contact details	
Name: Tim Jap	Position: Special Counsel
Branch: Governance, Ethics, & Integrity	Division: Office of General Counsel
	Email: <a href="mailto:governance@treasury.nsw.gov.au">governance@treasury.nsw.gov.au</a>

# Contents

## Preface 5

<b>1</b>	<b>About this policy .....</b>	<b>6</b>
1.1	Legal framework and guiding policies.....	6
1.2	Policy scope and exceptions .....	6
<b>2</b>	<b>Privacy Obligations and Risks .....</b>	<b>6</b>
2.1	What types of information concern privacy? .....	6
2.1.1	Personal and health information.....	6
2.1.2	Types of personal and health information held by NSW Treasury .....	7
2.1.3	Exclusions from personal and health information.....	7
2.2	Privacy Impact Assessment (PIA).....	8
2.2.1	Who will use privacy impact assessments?.....	8
2.2.2	What criteria to consider in preparation for a PIA .....	9
2.2.3	Information Protection Principles and Health Privacy Principles .....	10
<b>3</b>	<b>Roles and responsibilities of NSW Treasury Employees .....</b>	<b>13</b>
3.1	Privacy Coordinator.....	13
3.2	Privacy officers and champions .....	13
3.3	Treasury staff .....	14
<b>4</b>	<b>Obligations to making a privacy report .....</b>	<b>15</b>
4.1	Privacy incidents, complaints and Mandatory Notification of Data Breach (MNDB).....	15
4.2	Privacy report review process.....	15
<b>Appendix A:</b>	<b>Privacy Threshold Assessment Tool .....</b>	<b>16</b>
<b>Appendix B:</b>	<b>Privacy Impact Assessment (PIA).....</b>	<b>17</b>
<b>Appendix C:</b>	<b>Privacy Notice and consent text template for collecting personal information..</b>	<b>30</b>
<b>Appendix D:</b>	<b>Privacy Impact Assessment Process .....</b>	<b>31</b>
<b>Appendix E:</b>	<b>Making a privacy complaint (For internal review).....</b>	<b>32</b>
<b>Appendix F:</b>	<b>Privacy Report Process .....</b>	<b>34</b>
<b>Appendix G:</b>	<b>Draft letter to the NSW Privacy Commissioner regarding receipt of application for internal review under section 53 of the PPIP Act.....</b>	<b>37</b>
<b>Appendix H:</b>	<b>Types of personal and health information held by NSW Treasury.....</b>	<b>38</b>

# Preface

The NSW Treasury's Privacy Management Plan and Guidelines (the Plan), provides practical guidance for NSW Treasury staff on requirements of section 33 of the *Privacy and Personal Information Protection Act 1998* (the PPIP Act) for managing personal information.

At its position at the centre of government, NSW Treasury holds and uses a wide range of personal, private and confidential information. This information is integral to its function as the lead on economic, jobs and investment conversations.

The privacy rights of citizens, stakeholders, and staff are protected under the PPIP Act and the *Health Records and Information Privacy Act 2001* (the HRIP Act) which is reflected in the Plan.

The Plan supports NSW Treasury's commitment to open and accountable government in accordance with the *Government Information (Public Access) Act 2009* (the GIPA Act), while at the same time recognising the privacy rights of individuals. The Plan applies to all staff within NSW Treasury, to ensure privacy obligations are met to a high standard.

Michael Coutts-Trotter

Secretary

NSW Treasury

17 November 2023

## Note

General inquiries concerning this document should be initially directed to:

Office of General Counsel, NSW Treasury: [governance@treasury.nsw.gov.au](mailto:governance@treasury.nsw.gov.au).

This publication can be accessed from the Treasury's website [www.treasury.nsw.gov.au/](http://www.treasury.nsw.gov.au/).

# 1 About this policy

---

## 1.1 Legal framework and guiding policies

This Privacy Management Plan and Guidelines (PMP) has been developed in accordance with the *Privacy and Personal Information Protection Act 1998* (the PPIP Act), the *Health Records and Information Privacy Act 2002* (the HRIP Act) and the introduction of a Mandatory Notification of Data Breach (MNDB) scheme by the *Privacy and Personal Information Protection Amendment Act 2022*. All public agencies in New South Wales are required to have a privacy management plan under section 33 of the PPIP Act.

The PMP sets out:

- what types of information concern privacy
- how to manage personal and health information to meet our obligations
- who to contact if you manage personal and health information, or require guidance on privacy
- how to make a report on privacy complaints, incidents and data breaches under the PPIP Act.

This PMP documents our commitment to safeguarding information held by NSW Treasury and adopting stringent processes in reviewing privacy complaints and incident reporting.

This policy should be read in conjunction with

- [Information Protection Principles \(IPPs\)](#)
- [Health Privacy Principles \(HPPs\)](#)
- [TIPP 5.20 Data Breach \(Privacy\) Response Plan and Procedure](#)

---

## 1.2 Policy scope and exceptions

This plan applies to all NSW Treasury employees, contractors, and others who collect, use, store and disclose information on behalf of NSW Treasury.

# 2 Privacy Obligations and Risks

---

## 2.1 What types of information concern privacy?

### 2.1.1 Personal and health information

‘Personal information’ is defined in section 4 of the PPIP Act as:

‘Information or an opinion (including information or an opinion forming part of a database and whether or not in a recorded form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion.’

Personal information is information that identifies an individual. It could include:

- a record which may include names, addresses and other details about an individual
- photographs, images, video or audio footage
- fingerprints, blood or DNA samples.

Other sensitive personal information includes, for example, ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities, Trade Union membership.

‘**Health information**’ is defined in section 6 of the HRIP Act to include information or an opinion about an individual’s physical or mental health or a disability, future provision of health services and health services provided, organ donation, genetic information or healthcare identifiers.

## 2.1.2 Types of personal and health information held by NSW Treasury

NSW Treasury holds the personal or health information of NSW Treasury employees, and externally, members of the public, information collected by contractors and others on behalf of NSW Treasury.

For a full explanation of the types of personal and health information held by NSW Treasury, see Appendix H.

## 2.1.3 Exclusions from personal and health information

In section 4(3) of the PPIP Act and section 5(3) of the HRIP Act, personal and health information does not include:

- information relating to a person who has been dead for more than 30 years
- information contained in a publicly available publication
- information or an opinion referring to a person's suitability for employment as a public sector official.

### Information in a publicly available publication.

Information about named or identifiable people published in newspapers, books or the Internet, broadcast on radio or television, posted on social media such as Facebook, LinkedIn, or Twitter, or made known at a public event is not considered to be personal information under the Acts. Because such information is publicly available, it cannot be protected from use or further disclosure.

### Employment-related information.

Information or opinions referring to someone’s suitability for employment as a Treasury member of staff (such as selection reports and references for appointment or promotions, or disciplinary records) is not considered to be personal information under the Acts and is therefore excluded from the Acts’ protections.

Such information, however, is still stored, secured, used and disclosed by Treasury with the same care as if it were protected by the Acts.



## Other employee-related personal information is protected by the Acts.

For example, records or information about work activities, such as video or photographs of staff in their workplace, are protected and may only be used in compliance with the Acts' provisions.

Other examples of work-related personal and health information include vaccination status, staff training records, leave applications and attendance records. All these are within the scope of the definitions and are protected by the Acts.

## 2.2 Privacy Impact Assessment (PIA)

### 2.2.1 Who will use privacy impact assessments?

Before collecting personal or health information for a NSW Treasury project, review, or other policy deliverables, you will need to undertake a privacy impact assessment (PIA). The purpose of the PIA is to assess and consider any privacy issues before a project, review, or other policy deliverables are undertaken. A PIA template is available to undertake a PIA at Appendix A and B.

Examples of when to use the PIA template could include (but is not limited to) plans to collect:

- survey feedback from NSW Treasury staff, members or the public or stakeholders
- the health or vaccination status of NSW Treasury staff or stakeholders
- contact details and/or digital images at a stakeholder event.

This Privacy Impact Assessment (PIA) must be approved by any of the following officers:

- Secretary
- Deputy Secretaries/Senior Executive Band 3
- Executive Directors/Senior Executive Band 2
- Directors/Senior Executive Band 1
- Staff within the Office of General Counsel at the grade of 9/10 or above.

Once completed, you are to provide a copy of the approved PIA to NSW Treasury's Privacy Coordinator.

The PIA / PTA template must be used regardless of the project but not all fields require an answer. Should an exemption be required from both forms, an application would need to be made to the Secretary as to the reasons why the exemption is sort.

#### Collection tips:

- When designing an information collection form, ask yourself: *'do we really need each bit of this information?'*
- By limiting the collection of personal and health information to only what you need, it is much easier to comply with the principles.
- If collecting personal or health information about someone, collect it from that person directly to ensure accuracy and to obtain any permission for disclosure of the information.
- If you need to collect health and/or personal information from a third party, contact the Governance, Ethics, & Integrity Branch for more information. Any collection must follow the IPC's guidelines.
- Do not ask for information that is not relevant.
- Be mindful of whether you're asking for information that is safeguarded, such as about a person's ethnicity or race, political opinions, religious or philosophical beliefs, trade union



membership or sexual activities. Treat this information with extra care and seek advice before disclosing it.

- Individuals providing their personal or health information to NSW Treasury have a right to know the full extent of how the information they provide will be used, retained and disclosed, and to choose whether or not they wish to go ahead with providing information on that basis.
- Think about whether you are collecting personal or health information from people living in the European Union (EU) with an intention of providing goods and services to them. If so, you might be subject to the EU's General Data Protection Regulation (GDPR), in which case you should make sure your collection meets the requirements of Articles 13-14 of the GDPR. This includes if you are collecting information about and tracking web-based behaviour, where that behaviour is coming from the EU.

#### **2.2.1.1 Privacy Threshold Assessment tool (PTA)**

If you are unsure about privacy requirements for a specific project, a Privacy Threshold Assessment tool can help you decide if the information that you plan to collect has privacy concerns. For a copy of the form, see Appendix A.

#### **2.2.1.2 Privacy Impact Assessment (PIA)**

For a copy of the PIA template, see Appendix B.

### **2.2.2 What criteria to consider in preparation for a PIA**

#### **2.2.2.1 Collection**

When collecting personal information, NSW Treasury should send the person a Privacy Notice that tells them:

- whether the collection is required by law
- what the consequences will be if they do not provide the information
- what it will be used for
- who will hold/store the information (if not the Department)
- who else might receive the information from the Department
- how they can access or update/correct their information.

For a sample Privacy Notice, see Appendix C.

#### **2.2.2.2 Storage and security**

See Information Management policies:

- TIPP 4.01 Information and Records Management Framework
- TIPP 4.02 Information Creation, Capture, and Storage Policy
- TIPP 4.04 Information Access, Labelling, Handling, and Sharing Policy
- TIPP 4.09 Information Archiving and Disposal

#### **2.2.2.3 Use and disclosure**

You must always consider, how you are going to use the information, and further who you will disclose it to. For example, will this be given to external parties (including other NSW government departments)? If so, why do you need to disclose it to them, and should you choose to disclose, what are the safeguards?

#### 2.2.2.4 Managing privacy access requests

People have the right to access, amend and update personal information about them that NSW Treasury holds.

NSW Treasury must assist a person to find out what personal and health information it holds about them, and then provide access to this information without excessive delay. NSW Treasury does not charge any fees to access or amend personal or health information.

For members of the public, a request for access to any personal information held by NSW Treasury should be made in writing to the NSW Treasury Privacy Coordinator when their request cannot be dealt with on an informal basis. The Privacy Coordinator will allocate the matter to an officer no less senior than an associate director or equivalent within the line area that the Privacy Coordinator believes would hold the information requested and/or that needs amended.

Any person can make a formal application to the NSW Treasury Privacy Coordinator and this application should:

- include the person's name and contact details (postal address, telephone number and email address if applicable)
- explain what the person is seeking, such as whether the person is enquiring about the personal information held about them, or whether the person is wishing to access and amend that information
- if the person is seeking to access or amend their information:
  - explain what personal or health information the person wants to access or amend
  - explain how the person wants to access or amend it.

For all internal and external requests, NSW Treasury aims to respond in writing to formal applications within 20 working days and will advise the applicant how long the request is likely to take, particularly if it may take longer than expected.

If an individual believes that NSW Treasury is taking an unreasonable amount of time to respond to an application, they have the right to seek an Internal Review.

Before seeking an Internal Review, we encourage individuals to first contact NSW Treasury to request provision of an update or timeframe. Alternatively, should you have any concerns or wish to raise any issues on an informal basis, please contact the privacy coordinator on the contact details below.

NSW Treasury encourages staff wanting to access or amend their own personal or health information to use the available self-service platforms or contact HR Division.

#### 2.2.2.5 PIA assessment process

For the full PIA process, see Appendix D

### 2.2.3 Information Protection Principles and Health Privacy Principles

#### Applying the privacy principles in NSW

Sections 8 to 19 of the PPIP Act and Schedule 1 to the HRIP Act set the privacy standards public sector agencies are expected to follow when dealing with personal information. Twelve information protection principles (IPPs) govern the collection, retention, accuracy, use and disclosure of personal information, including rights of access and correction.

Below is an overview of the IPPs as they apply to NSW Treasury:

12 Information Protection Principles		
<b>Collection</b>	1.	Lawful – We only collect personal information for a lawful purpose that is directly related to our functions and activities and necessary for that purpose.
	2.	Direct – We collect personal information directly from the person concerned.
	3.	Open – When collecting personal information, we inform people why their personal information is being collected, what it will be used for, to whom it will be disclosed, how they can access and amend it and any possible consequences if they decide not to give it to us.
	4.	Relevant – When collecting personal information, we ensure it is relevant, accurate, up-to-date and not excessive, and does not unreasonably intrude into peoples' personal affairs.
<b>Storage</b>	5.	Secure – We store personal information securely, keep it no longer than necessary, destroy it appropriately, and protect it from unauthorised access, use, modification or disclosure.
<b>Access</b>	6.	Transparent – We explain what personal information is stored, what it is used for and peoples' right to access and amend it.
	7.	Accessible – We allow people to access their own personal information without unreasonable delay or expense.
	8.	Correct – We allow people to update, correct or amend their personal information where necessary.
<b>Use</b>	9.	Accurate – We make sure that personal information is relevant and accurate before using it.
	10.	Limited – We only use personal information for the purpose it was collected for unless the person consents to the information being used for an unrelated purpose.
<b>Disclosure</b>	11.	Restricted – We will only disclose personal information with people's consent unless they were already informed of the disclosure when the personal information was collected.
	12.	Safeguarded – We do not disclose sensitive personal information (such as ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities, or trade union membership) without consent.

**Schedule 1 to the HRIP Act** provides a similar set of privacy standards for health information. They are the health privacy principles (HPPs) and they are largely the same as the IPPs. Some additional obligations and standards apply, instead of IPP 12 for safeguarded information.

An overview follows below on how the HPPs apply to NSW Treasury:

12 Health Privacy Principles		
<b>Collection</b>	1.	Lawful – We only collect health information for a lawful purpose that is directly related to our functions and activities and necessary for that purpose.
	2.	Relevant – When collecting health information, we ensure it is relevant, accurate, up-to-date and not excessive, and does not unreasonably intrude into peoples' personal affairs.
	3.	Direct – We collect health information directly from the person concerned unless it is unreasonable or impractical to do so.

	4.	Open – When collecting health information, we inform people why their health information is being collected, what it will be used for, to whom it will be disclosed, how they can access and amend it and any possible consequences if they decide not to give it to us.
<b>Storage</b>	5.	Secure – We store health information securely, keep it no longer than necessary, destroy it appropriately, and protect it from unauthorised access, use or disclosure.
<b>Access</b>	6.	Transparent – We provide details on the health information that is stored, what it is used for and peoples’ right to access and amend it.
	7.	Accessible – We allow people to access their own health information without unreasonable delay or expense.
	8.	Correct – We allow people to update, correct or amend their health information where necessary.
<b>Use</b>	9.	Accurate – We make sure that health information is relevant and accurate before using it.
	10.	Limited – We only use health information for the purpose it was collected for unless: <ul style="list-style-type: none"> <li>(a) the person has consented to its use for another purpose</li> <li>(b) it is being used for a purpose directly related to the purpose it was collected for</li> <li>(c) we believe that there is a serious threat to health or welfare</li> <li>(d) it is for the management of health services, training, research or to find a missing person</li> <li>(e) it is for law enforcement or investigative purposes.</li> </ul>
<b>Disclosure</b>	11.	Restricted – We only disclose health information for the purpose it was collected for unless: <ul style="list-style-type: none"> <li>(a) the person has consented to its disclosure for another purpose</li> <li>(b) it is being disclosed for a purpose directly related to the purpose it was collected for</li> <li>(c) we believe that there is a serious threat to health or welfare</li> <li>(d) it is for the management of health services, training, research or to find a missing person</li> <li>(e) it is for law enforcement or investigative purposes.</li> </ul>
<b>Other</b>	12.	Identifiers – We do not use unique identifiers for health information, as they are not needed to carry out Treasury’s functions.
	13.	Anonymity – We allow people to stay anonymous if it is lawful and practical for them to do so.
	14.	Transborder – We do not usually transfer health information outside of New South Wales.
	15.	Linkage – We do not currently use a health records linkage system and do not anticipate using one in the future. But if we were to use one in the future, we would not do so without people’s consent.

## 3 Roles and responsibilities of NSW Treasury Employees

---

### 3.1 Privacy Coordinator

The Privacy Coordinator has three key roles:

1. **Advice and support:**
  - a. Providing privacy advice, about handling personal information, responding to complex enquiries from the Privacy Champions and Officers,
  - b. Assisting Privacy Champions and Officers with regards to Privacy Impact Assessments (PIAs) where there are complex issues raised,
  - c. Co-ordinating NSW Treasury's response to suspected or confirmed privacy data breaches
2. **Strategic initiatives:**
  - a. Working with relevant stakeholders in completing or coordinating privacy audits or other assurance activities at NSW Treasury to check that it is meeting its privacy obligations,
  - b. Drafting or reviewing privacy documentation, such as privacy policies and collection notices,
  - c. Identifying opportunities to improve privacy practices,
  - d. Coordinating privacy training, and other activities to promote privacy awareness for staff
3. **Liaison Officer between NSW Treasury, the Privacy Commissioner's Office and members of the public when it comes to Internal Reviews:**
  - a. Responding to queries about NSW Treasury's privacy practices from members of the public,
  - b. Handling privacy complaints that NSW Treasury receives directly. This may include investigating whether NSW Treasury has interfered with someone's privacy and trying to resolve the complaint,
  - c. Liaising with IPC and Office of the Australian Information Commissioner (OAIC) about data breach notifications, privacy complaints or significant projects,
  - d. Assessing whether requests from other organisations to share personal information that NSW Treasury holds are permitted under privacy law.

The role of Privacy Coordinator within NSW Treasury is undertaken by the Special Counsel and Lead Associate Director, Governance, Ethics, & Integrity (GE&I) within the Office of General Counsel.

---

### 3.2 Privacy officers and champions

Privacy Champions and Officers support NSW Treasury's privacy management plan by:

1. **Providing Advice and Approval**

- a. Providing advice to their groups about handling personal information, responding to general enquiries from their teams,
- b. Support and approve PIAs and where necessary escalate to the Privacy Coordinator for any complex PIAs that rise complex and/or novel issues,
- c. Work with the Privacy Coordinator and their teams to respond to suspected or confirmed privacy data breaches

## 2. Strategic Initiatives

- a. Raise and promote awareness of privacy and privacy best practices,
- b. Identify opportunities and champion privacy at their respective Extended Leadership Team (ELT) meetings
- c. Work with their teams and the privacy coordinator at reviewing privacy documentation
- d. Provide and/or coordinate privacy training for their teams

## 3. Be the face of privacy for their group

- a. Responding to queries from their teams on privacy
- b. Handling privacy complaints that have been referred to them by the privacy coordinator. This may include investigating whether NSW Treasury has interfered with someone's privacy and trying to resolve the complaint,
- c. Assist the privacy coordinator with any queries or requests from the IPC and/or the OAIC,
- d. Be the main point of contact for their team members on any privacy matters.

Privacy Champions hold the rank of Public Service Senior Executive Band 1 or above who have been nominated by their Deputy Secretary to undertake this function.

Privacy Officers are all legally qualified staff within the OGC, and the Associate Director, Information Access.

---

## 3.3 Treasury staff

All Treasury staff are required to follow the Privacy Management Plan and all the requirements stated. Staff should contact their Privacy Champion, or the privacy coordinator should they require further assistance.

## 4 Obligations to making a privacy report

---

### 4.1 Privacy incidents, complaints and Mandatory Notification of Data Breach (MNDB)

#### Privacy complaint

##### When to make a report

A breach of an individual's privacy is where a breach of one or more of the IPPs or HPPs has occurred.

An individual who considers his or her privacy has been breached can contact NSW Treasury to try and resolve the issue informally. Alternatively, or if no informal resolution can be reached, individuals can also make a complaint to NSW Treasury under section 53 of the PPIP Act and request a formal internal review of NSW Treasury's conduct in relation to the privacy matter (Internal Review).

##### How to make a report

For the full form and process to make a complaint, see Appendix E.

#### Mandatory Notification of Data Breach (MNDB)

A data breach occurs when information is subject to unauthorised access or disclosure, or when information is lost where the loss is likely to result in unauthorised access or disclosure due to human error, system failure or malicious or criminal attack.

##### When to make a report?

It is mandatory to make a report when you become aware of an actual or suspicious data breach to personal information held by Treasury, including some personal information that is held by contracted service providers.

##### How to make a report

For steps to be followed and practical guidance in a data breach, the Data Breach (Privacy) Response Plan and Procedure TIPP5.20 is available for access to NSW Treasury employees. It includes specific security controls and operational protocols.

---

### 4.2 Privacy report review process

The Privacy Coordinator is responsible for receiving, allocating and overseeing Internal Reviews in relation to privacy matters. For a full explanation of the process, see Appendix F.



## Appendix A: Privacy Threshold Assessment Tool

When you are unsure if the information that you collect has privacy concerns, fill in this Rapid Privacy Threshold Assessment and send it to [governance@treasury.nsw.gov.au](mailto:governance@treasury.nsw.gov.au)

New South Wales Treasury's Privacy team, Governance, Ethics and Integrity (GE&I) Branch in the Office of General Counsel will review your responses to confirm whether a complete Privacy Impact Assessment (Appendix B) is required. The Privacy team may contact you for further information or clarification.

Rapid Privacy Threshold Assessment		
Project Outline		
1	Name of project	
2	Project aim	
3	Associated existing programs or projects, if applicable	
4	Business unit responsible for the project	
5	Contact name (person completing this Rapid Privacy Threshold Assessment form)	
6	Project manager	
7	Director	
8	Executive Director	
Rapid Privacy Threshold Assessment		
9	Does the program or event involve personal information?	
10	Does the program or event involve other information that has the potential to identify individuals?	
11	Does the program or event involve sensitive information?	
12	Does the program or event involve health information?	
13	Does the program or event involve information that has previously been de-identified?	
14	Describe the information that is being collected and how it is going to be presented?	

## Appendix B: Privacy Impact Assessment (PIA)

Use this mandatory Privacy Impact Assessment when 1) you are advised by the New South Wales Treasury's Privacy team to do one, following the outcome of your Rapid Privacy Threshold Assessment (Appendix A), and 2) you and your team collect, use, store and disclose personal or health information.

Date of PIA:			
Status (New or Amendment):			
Prepared by:			
Position:			
Email:		Telephone Number:	

### a. Scope of this privacy impact assessment

The (name of line area) has prepared a Privacy Impact Assessment.

The Privacy Impact Assessment has been undertaken by...

### b. Applicable legislation

This PIA analyses the privacy impacts of collecting, storing, using, and disclosing personal information against the privacy principles set out in the following legislation:

- *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**).
- *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**)
- *Data Sharing (Government Sector) Act 2015* (NSW) (**Data Sharing Act**).

### c. Stakeholders Consulted

Stakeholder	Internal/External	Scope of Consultation	Method	Response

## Project Outline

Purpose	
Operational Objective (why are you collecting it?)	
Personal / Sensitive Information (Name/DOB/Address/TFN other identifiers)	

## Collection – IPPs 1 – 4

Questions	Responses
<ol style="list-style-type: none"><li>1. Is all the personal information collected necessary for the program?</li><li>2. Do you need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?</li><li>3. If individuals can remain anonymous, will you be collecting indirect identifiers, such as demographic information?</li><li>4. How will the personal information be collected?</li><li>5. Is the personal information collected directly from the individual?</li><li>6. Will the individual be notified about the collection of their personal information?</li></ol>	

7.	Will any personal information about the individual be collected indirectly from another source?	
8.	Will the individual be notified that their personal information has been collected from another source?	
9.	Will the program assign a unique identifier or collect a unique identifier assigned by another organisation to adopt as your organisation's own?	
10.	Does the program require an individual to provide a unique identifier?	
11.	What steps will you take to ensure the personal information collected is accurate, complete, and up to date?	

#### Storage, Retention & Security – IPPs 5 – 8

Questions		Responses
12.	Are there security measures in place (existing or intended) to protect the personal information collected and used for this program?	
13.	Where and how will personal information be stored?	
14.	Who will have access to the personal information?	
15.	Have you completed a separate security risk assessment?	
16.	How will you ensure the ongoing accuracy, completeness, and currency of the personal information used in this program?	
17.	Is there a way for a person to find out the types of personal information your organisation holds about them?	

18.	Can you tell them the purposes for which it is held, and how your organisation collects, holds, uses and discloses that information?	
19.	How can individuals request access to, or correct their personal information?	
20.	How long will the personal information be kept for?	
21.	How will personal information be destroyed once it is no longer required?	
22.	If applicable, what will happen to personal information held by third parties (such as contracted service providers, cloud storage, third party platforms etc.)?	

#### Use & Disclosure – IPPs 9 – 12

Questions		Responses
23.	Is the personal information involved in this program used or disclosed for the main or primary purpose for which it was collected?	
24.	Does the program use or disclose personal information for a new or additional purpose other than the original purpose of collection?	
25.	Will the individual be notified of the additional use(s) of their personal information?	
26.	Does the program use or disclose a unique identifier assigned by another organisation?	
27.	Will any data matching occur as part of this program? This includes matching datasets within the	

28.	program, or matching to other datasets external to the program. Will any personal information be de-identified as part of the program?	
-----	---	--

#### Other Requirements – Privacy Act (Cth), TFN Rule, PPIP Act and HRIP Act

Questions		Responses
29.	Will any personal information be shared outside of your organisation?	
30.	Will any personal information be transferred outside New South Wales?	
31.	Who can individuals complain to if they have concerns about the handling of their personal information?	
32.	Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this program?	
33.	Will the program be evaluated against its objectives?	
34.	Does the program comply with your organisation's other information handling or information management policies?	
35.	Will this PIA be published?	
36.	Are there any other broader privacy considerations associated with this program?	

## Risk Analysis

The following table summarises each privacy principle's essential requirements to help detect potential privacy problems.

Risk Name	Risk Detail	Controls	Inherent Risk			Residual Risk
			Likelihood	Impact	Rating	Rating
For example: Treasury Data will be stored overseas	(Describe the Risk) - For example - according to the terms of the service, the data will be stored on multiple servers from different countries	(What controls have you decided to help mitigate the risk) - For example: We have limited the data to only be stored on EU servers / or We've amended the terms so that data can only be stored in Australia	(how likely refer to Treasury's Risk Framework ) For example: Possible	For example : Significant	For Example: Significant	(After the controls, what's the risk now) - For example: Moderate



**Privacy Officer**

Having reviewed the responses above, I am satisfied that a Privacy Impact Assessment is:

- ☐ Satisfactory
- ☐ Not Satisfactory

<b>Name:</b>			
<b>Position:</b>			
<b>Signed:</b>		<b>Date:</b>	

Comments:

Delegate Approval (PSSE B1/B2/B3 or a Clerk 11/12 within the Office of General Counsel)

<b>Name:</b>			
<b>Position:</b>			
<b>Approved / Not Approved</b>			
<b>Signed:</b>		<b>Date:</b>	

---

## Appendix C: Privacy Notice and consent text template for collecting personal information

The following **Template privacy notice** can be used when collecting personal information in a written form. However, this is a template only, and teams should still seek the advice of the Privacy Coordinator to ensure the privacy notice is appropriate in each case.

### Template privacy notice

The information you have provided has been collected for the purpose of *[insert purpose of collection, noting that this will also determine the purpose for which the information can be lawfully used and disclosed]*. Providing us with the requested information is/is not required by law. However, if you choose not to provide us with the requested information, ... *[describe the main consequences for person if information is not provided – e.g. NSW Treasury cannot investigate your complaint]*.

You may request access to your information at any time. To access or update your personal information, or for more information on our privacy obligations, ask to speak to the NSW Treasury Privacy Coordinator who can be contacted at [governance@treasury.nsw.gov.au](mailto:governance@treasury.nsw.gov.au).

*[insert the following highlighted paragraph **only** where the Department wishes to use or disclose Personal Information for a secondary purpose not directly related to the primary purpose for which the information was collected.]*

With your permission, we would also like to *[use/disclose]* your information to: *[describe here the intended secondary purpose – e.g. put you on your mailing list for future community events]*.

☐ I consent to my personal information being *[used / disclosed]* for the purpose of *[name the secondary purpose]*.

Signature:

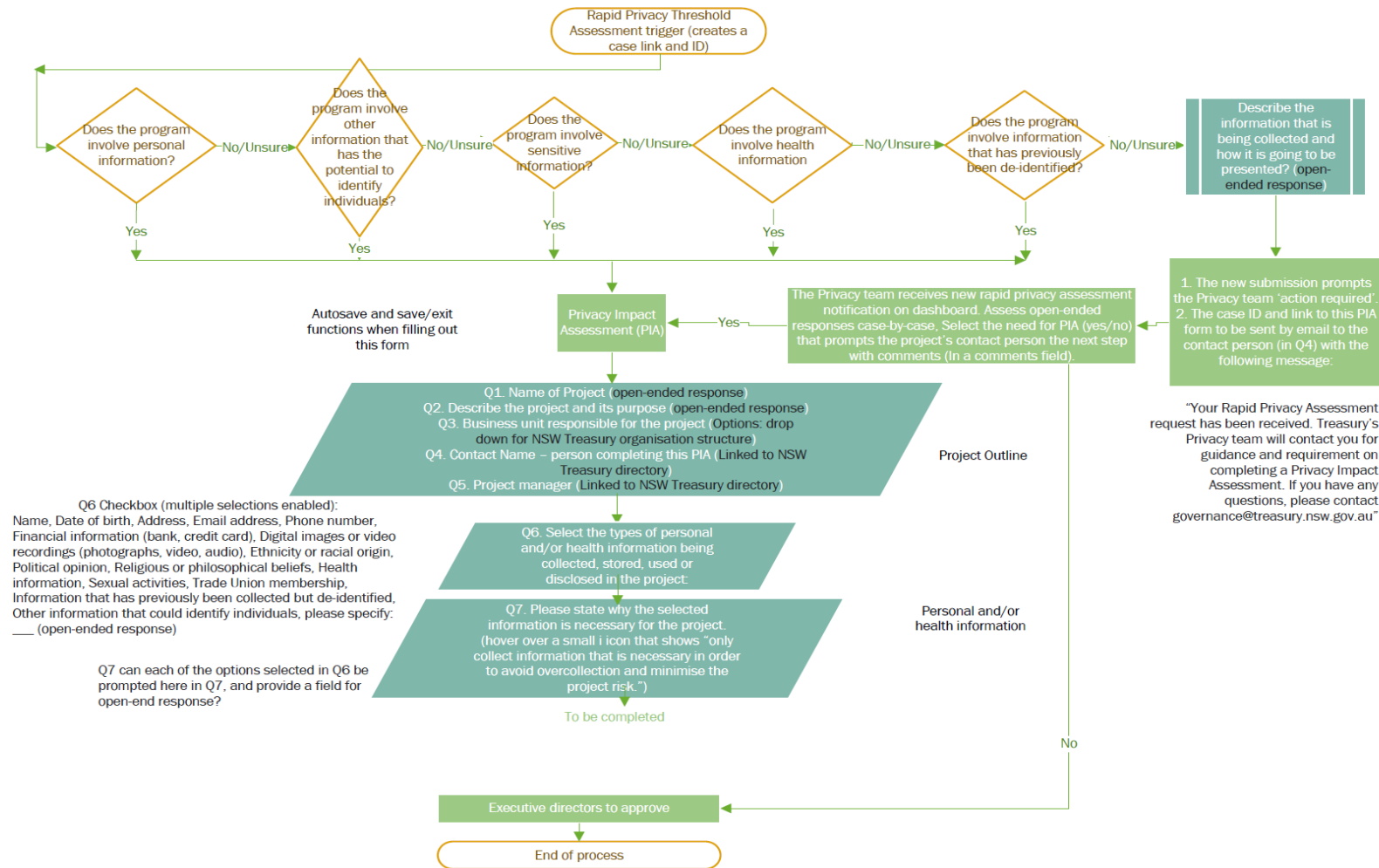
If personal information is being collected verbally, see **Verbal collections** below.

### Verbal collections

When collecting Personal Information verbally (e.g. during telephone discussions), we can use less formal wording, so long as we explain *how* the person's Personal Information will be used, *and to whom else* it will likely be disclosed. If the person asks further questions about whether the information is really needed, then we can go into more depth, and we can also mention their access and amendment rights or offer to let them speak to Treasury's Privacy Coordinator.

However if we need to obtain the person's verbal consent to a secondary use or disclosure, we must explain what it is we are asking, and we must ensure that they understand they are free to say 'no'. We must also make a file-note of what was said.

## Appendix D: Privacy Impact Assessment Process



## Appendix E: Making a privacy complaint (For internal review)

Please complete this form to apply for a review of conduct under section (select one):

☐ 53 of the **Privacy and Personal Information Protection Act 1998** (the PPIP Act)

☐ 21 of the **Health Records and Information Privacy Act 2002** (the HRIP Act)

If you need help filling out this form, please contact the Privacy Coordinator on 02 9228 4077 or visit the Information & Privacy Commission website at [www.ipc.nsw.gov.au](http://www.ipc.nsw.gov.au).

1	Name of the agency you are complaining about: NSW Treasury
2	Your full name: Click or tap here to enter text.
3	Your postal address: Click or tap here to enter text. Telephone number: Click or tap here to enter text. Email address: Click or tap here to enter text.
4	If the complaint is on behalf of someone else, please provide their details: Click or tap here to enter text. What is your relationship to this person (e.g., parent)? Click or tap here to enter text. Is the person capable of making the complaint by himself or herself? <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> unsure
5	What is the specific conduct you are complaining about? (‘Conduct’ can include an action, a decision, or even inaction by the agency. For example, the ‘conduct’ in your case might be a decision to refuse you access to your personal information, or the action of disclosing your personal information to another person, or the inaction of a failure to protect your personal information from being inappropriately accessed by someone else.) Click or tap here to enter text.
6	Please tick which of the following describes your complaint: (you may tick more than one option) <input type="checkbox"/> collection of my personal or health information <input type="checkbox"/> security or storage of my personal or health information <input type="checkbox"/> refusal to let me access or find out about my own personal or health information <input type="checkbox"/> accuracy of my own personal or health information <input type="checkbox"/> use of my personal or health information <input type="checkbox"/> disclosure of my personal or health information <input type="checkbox"/> other <input type="checkbox"/> unsure
7	When did the conduct occur (date)? (Please be as specific as you can) Click or tap here to enter text.
8	When did you first become aware of this conduct (date)? Click or tap here to enter text.

9	<p>You need to lodge this application within six months of the date at question 8. If more than six months have passed, you will need to ask Treasury's Privacy Coordinator for special permission to lodge a late application. If you need to, write here to explain why you have taken more than 6 months to make your complaint:</p> <p><i>Click or tap here to enter text.</i></p>
10	<p>What effect did the conduct have on you?</p> <p><i>Click or tap here to enter text.</i></p>
11	<p>What effect might the conduct have on you in the future?</p> <p><i>Click or tap here to enter text.</i></p>
12	<p>What would you like to see NSW Treasury do about the conduct? (for example: an apology, a change in policies or practices, your expenses paid, damage paid to you, training for staff, etc.)</p> <p><i>Click or tap here to enter text.</i></p>
13	<p>I understand that this form will be used by NSW Treasury to process my request for an Internal Review.</p> <p>I understand that details of my application will be referred to the NSW Privacy Commissioner as required by law, and that the Privacy Commissioner will be kept advised of the progress of her review.</p> <p>I would prefer the Privacy Commissioner to have:</p> <p><input type="checkbox"/> a copy of this application form, or</p> <p><input type="checkbox"/> just the information provided at questions 5-12.</p>

### Applicant's signature and lodgement

Applicant's signature: ..... Date: .....

---

Please post this form to:

Special Counsel  
 Governance, Ethics, & Integrity  
 Office of General Counsel  
 NSW Treasury  
 GPO Box 5469, Sydney NSW 2001

Please keep a copy for your own records

## Appendix F: Privacy Report Process

### Internal Review

The Privacy Coordinator is responsible for receiving, allocating and overseeing Internal Reviews in relation to privacy matters. The Privacy Coordinator provides a single point of contact for individuals seeking further information on how NSW Treasury complies with the Acts. The Privacy Coordinator will receive all correspondence and enquiries regarding the Acts, including any Internal Review requests.

The Privacy Coordinator's role also includes monitoring, recording and reporting on the progress of all Internal Review applications received.

Within NSW Treasury, the responsibilities of the Privacy Coordinator are currently held by the Special Counsel, Governance, Ethics, & Integrity.

The Privacy Coordinator will designate an officer within NSW Treasury to be the delegated officer (at a minimum an officer who is employed at the Senior Executive Services Band 1 or above) for the purposes of conducting the Internal Review under the PPIP Act.

Internal Reviews will generally be conducted by a delegated officer with no involvement in the matter giving rise to the complaint of breach of privacy (the Reviewing Officer). The delegated officer may seek legal or other assistance in conducting the review, including from the Privacy Coordinator, a privacy officer, and/or the Governance, Ethics, & Integrity Branch.

Under section 54(1) of the PPIP Act, NSW Treasury is required to notify the NSW Privacy Commissioner of the receipt of an application for an Internal Review of conduct and keep the NSW Privacy Commissioner informed of the progress reports of the Internal Review. In addition, the NSW Privacy Commissioner is entitled to make submissions to NSW Treasury in relation to the application for Internal Review (section 54(2) of the PPIP Act).

Under section 53(6) of the PPIP, an Internal Review must be completed within 60 days of the receipt of the application.

Under section 53(8) of the PPIP Act, as soon as practicable, or in any event within 14 days, after the completion of the Internal Review, NSW Treasury must inform the applicant of all of the following:

- findings of the review (and the reasons for those findings)
- action proposed to be taken by NSW Treasury (and the reasons for taking that action)
- the right of the person to have those findings, and NSW Treasury's proposed action, administratively reviewed by the NSW Civil and Administrative Tribunal (NCAT).

When NSW Treasury receives an Internal Review, the Privacy Coordinator will send both:

- an acknowledgment letter to the applicant and advise that if the Internal Review is not completed within 60 days, they have a right to seek a review of the conduct by NCAT
- a letter to the NSW Privacy Commissioner with details of the application and a photocopy of the written complaint.

There is an example of a letter of notification to the Privacy Commissioner of receipt of request for an Internal Review at Appendix G.

The Reviewing Officer responsible for completing the final determination must consider any relevant material submitted by the applicant or the NSW Privacy Commissioner. Before completing the Internal Review, the Reviewing Officer should send a draft copy of the preliminary determination to the NSW Privacy Commissioner to invite any submissions.

NSW Treasury follows the model of the Internal Review process provided by the NSW Information and Privacy Commission which can be found at <https://www.ipc.nsw.gov.au/privacy/agencies/how-handle-internal-review>.

In finalising the determination, the Reviewing Officer will prepare a report containing their findings and recommended actions.

NSW Treasury may:

- take no further action on the matter
- make a formal apology to the applicant
- take appropriate remedial action, which may include the payment of monetary compensation to the applicant
- undertake that the conduct will not occur again
- implement administrative measures to ensure that the conduct will not occur again.

The Reviewing Officer will notify the applicant in writing of some or all of:

- the findings of the review
- the reasons for the finding, described in terms of the IPPs and/or the HPPs
- any action NSW Treasury proposes to take
- the reasons for the proposed action (or no action)
- their entitlement to have the findings and the reasons for the findings reviewed by NCAT.

### **Recording of Internal Reviews**

NSW Treasury records all applications for Internal Review in a secure Objective file and workflow. The workflow tracks the progress of the Internal Review process and the determination of the completed review.

The details recorded in this system will provide the statistical information on Internal Review applications to be included in NSW Treasury's Annual Report.

### **External Review**

#### **Complaints to the NSW Privacy Commissioner**

Any individual who considers that their privacy has been breached can make a complaint to the NSW Privacy Commissioner under section 45 of the PPIP Act without first going through the Internal Review process of NSW Treasury. The complaint must be made within 6 months (or such later time as the NSW Privacy Commissioner may allow) from the time the individual first became aware of the conduct or matter the subject of the complaint.

However, the NSW Privacy Commissioner can decide not to deal with the complaint if it would be more appropriately dealt with as an Internal Review by NSW Treasury (section 46(3)(e) of the PPIP Act).

#### **Administrative Review by NCAT**

If the applicant is not satisfied with the outcome of NSW Treasury's Internal Review, they may apply to NCAT to review the decision. If NSW Treasury has not completed the Internal Review within 60 days, the applicant can also take the matter to NCAT.

A person must seek an Internal Review before they have the right to seek an administrative review by NCAT (section 55(1) of the PPIP Act).

To seek review by NCAT, the individual must apply within 28 days from the date of the Internal Review decision or within 28 days of the Internal Review not being completed within 60 days.

NCAT has the power to make binding decisions (section 55(2) of the PPIP Act).



For more information including current forms and fees, please contact NCAT:

website: <https://www.ncat.nsw.gov.au/>  
phone: 1300 006 228  
post: PO Box K1026, Haymarket NSW 1240  
visit: NSW Civil and Administrative Tribunal  
Administrative and Equal Opportunity Division  
Level 10 John Maddison Tower  
86-90 Goulburn Street  
Sydney NSW 2000

NCAT cannot give legal advice; however, the NCAT website has general information about the process it follows and legal representation.

## Appendix G: Draft letter to the NSW Privacy Commissioner regarding receipt of application for internal review under section 53 of the PPIP Act

(NSW Treasury letterhead) File number:

Date

[Insert name of current Privacy Commissioner]

NSW Privacy Commissioner GPO Box 7011

Sydney NSW 2001

Dear [insert name of current Privacy Commissioner],

**Notification in accordance with s. 54(1) of the NSW *Privacy and Personal Information Protection Act 1998*.**

NSW Treasury has received an application for Internal Review under s. 53 of the *Privacy and Personal Information Protection Act 1998*. A copy of the letter of application is attached.

The matter is being investigated. I shall keep you informed of the progress and outcome of the review.

Should you have any submissions regarding this matter, please send them to me at the above address.

Yours sincerely,

(Name of Occupant)

**Special Counsel**

**Governance, Ethics, & Integrity**

## Appendix H: Types of personal and health information held by NSW Treasury

**Employee records** NSW Treasury and contracted service providers (such as GovConnect, Contractor Central, myCareer, Department of Planning and Environment (DPE)) hold a range of NSW Treasury employee records (including for contractors, and secondees). This information includes, but is not limited to:

- records of dates of birth, addresses and contact details (including emergency contacts)
- payroll (including Superannuation), attendance and leave records (including medical certificates)
- performance management and evaluation records
- training records
- flexible working arrangements
- workers compensation records
- vaccination status
- work health and safety records
- records for equal employment opportunity reporting purposes.

An employee or contractor of NSW Treasury may access most of their records via self-service platforms (such as SAP or Cornerstone). They can also access the entirety of their own file under the supervision of HR staff.

Apart from the employee or contractor the file relates to, authorised access is provided to the members of the Human Resources team at NSW Treasury, service providers (such as GovConnect, Contractor Central, myCareer, Department of Planning and Environment (DPE)) and appointed Audit officers.

Employee records are stored in soft copy in the Human Resources systems and Objective files maintained by the respective service providers. This includes leave records, payroll processing information, leave accruals, medical certificates, and parental leave information.

HR also maintains separate personnel files in the Objective document management system for all current and former employees. These files include some contracts, remuneration details, and any ongoing cases being managed by HR (such as conduct investigations and WorkCover claims). Access to these personnel files is controlled and limited only to authorised HR employees.

NSW Treasury has an agreement with GovConnect, managed through the Department of Customer Service, that affects how GovConnect handles employee records in the SAP and Objective systems.

The Service Partnership Agreement between NSW Treasury and GovConnect confirms that GovConnect will have access to information from and about NSW Treasury in the course of business, and that GovConnect is bound to comply with the Acts.

The Service Partnership Agreement (SPA) between NSW Treasury and Department of Planning and Environment confirms that DPE will manage Treasury's Information Management obligations including privacy relating to the Office of Energy and Climate Change (OECC). When handling information from OECC, DPE is required to comply as if it were in Treasury's position.

Employee records are also held in relation to commercial assets that have now been sold by the State. These are primarily archived hard copy records, a register of which is kept electronically with access restricted only to the relevant business areas.

### **Information collected relating to conflict of interest**

NSW Treasury staff are required to disclose any actual, potential or perceived conflicts of interest as part of the onboarding process. This information is reviewed and updated regularly, and as any conflicts arise or change. Information of this nature will primarily be stored on Protecht, Treasury's Risk Management System.

NSW Treasury branches may also keep secure copies of NSW Treasury staff disclosures on emails, or other secure NSW Treasury systems. Regardless of where they store the information, they are subject to the same requirements under this plan.

Examples may include, line areas keeping an excel spreadsheet with people's conflicts of interest, a manager may maintain an email folder within their outlook, and/or placing it in a secure OneDrive that is accessible only to the manager. Regardless, as mentioned above, should line areas choose to keep this information, they will need to comply with this policy.

## **5 Digital images**

NSW Treasury holds digital images of all staff members. These are used to produce staff identification cards and other internal purposes including publication on Treasury's intranet.

NSW Treasury may also hold digital images of senior and/or board members of government-owned businesses that are used for onboarding and other internal and external purposes including publication on Treasury's intranet and webpage.

NSW Treasury may also collect and hold digital images obtained from industry or other third-party events, which may be used for other internal and external purposes.

NSW Treasury may also collect and hold digital images of people from various stakeholders requesting a meeting with the cluster ministers or through correspondence such as emails, and letters with their digital image.

NSW Treasury may also hold digital images collected from social platforms, where staff or participants have voluntarily provided these to participate in social and wellbeing events.

For events, NSW Treasury staff are required to inform attendees that digital images of the event may be used in NSW Government publications and any other internal and external purposes.

Any further use or reproduction of non-public digital images collected and held by NSW Treasury must be in accordance with the stated purpose provided by NSW Treasury (such as the publication of staff or board member images) unless the relevant individual has approved their use for other purposes. This personal information must also be held and used in accordance with other relevant NSW Treasury policies and protocols for record-keeping and intellectual property.

## **6 Contact details**

NSW Treasury holds contact details of various third parties that are in the public domain and not in the public domain, including for:

- government agency CEOs, senior executives, members of inter-departmental, and members of inter-government, working groups and similar, members of government boards and advisory committees
- stakeholders participating in stakeholder consultation forums
- inviting stakeholders to participate in NSW Treasury's consultation forums
- businesses and individuals involved in NSW Treasury's programs and schemes

- businesses and individuals attending NSW Treasury-hosted events and some business familiarisation programs
- businesses and individuals that have registered for NSW Treasury newsletters and collaboration/networking platforms
- businesses and individuals that are registered on NSW Treasury-hosted procurement systems
- businesses and individuals that are suppliers on NSW Treasury-managed contracts and schemes
- businesses and individuals that have applied to NSW Treasury and/or other departments where NSW Treasury holds policy responsibilities, for funding, grants or other assistance or services
- businesses and individuals that have responded to a call for submissions on a particular project
- people participating in surveys and community engagement events
- people who write or are referred by other ministers, to the Treasury ministers, where these contact details have been forwarded for a response
- people who have made a complaint, enquiry, compliment or suggestion through NSW Treasury's websites or other mechanisms
- people who have made formal access applications under the GIPA Act.

NSW Treasury often uses information in the public domain to contact people in relation to NSW Treasury work and invite them to relevant meetings and events.

By contrast, when NSW Treasury collects personal (non-public) information, such as private contact details, NSW Treasury staff **must** clearly disclose the purpose for collecting the information, how it will be used – and must only use the information for the disclosed purpose unless an individual has agreed to be contacted for additional reasons.

The disclosed purpose may be to invite an individual to a meeting or event. NSW Treasury may also ask individuals providing personal information if they would like to be invited to similar events in the future, updated on similar issues, and receive NSW Treasury communications such as emails, newsletters and social media alerts.

## **7 NSW Treasury must only use personal information for the purpose collected – unless an individual has agreed to additional uses**

For example, when an individual provides personal information such as private contact details to NSW Treasury as part of an enquiry, those contact details will only be used in managing and responding to that enquiry.

They will not be used for any other purpose such as unrelated marketing purposes, (to promote attendance at an unrelated event for example) unless the individual expressly consented to other uses of their personal information.

However, if the individual's contact details are publicly available, NSW Treasury may use the public domain information to contact them, such as inviting them to an event.

For clarity, NSW Treasury branches should record when contact details contained in consolidated stakeholder consultation lists, is sourced from public domain information.

## **8 Employee health Information for hybrid working arrangements**

NSW Treasury may receive and hold information about the health and personal circumstances of NSW Treasury employees (including contractors), provided by employees in relation to hybrid working arrangements. NSW Treasury stores such health information securely, typically on MS Teams.

## 9 Identification documents

In some cases, NSW Treasury may hold identification documents for certain individuals. These documents are usually collected where individuals are required to prove their identity or vaccination status, to access certain services or programs of NSW Treasury and are attached to the application, email, or form. Proof of identity documents may also be required when making applications for information under the GIPA Act or the PPIP Act.

## 10 Correspondence records

NSW Treasury holds the following correspondence records:

- contact details of people who have written to or emailed NSW Treasury or responsible Ministers, referrals from other ministers and department, either on their own behalf or others
- contact details of people who have made a complaint, enquiry, compliment or suggestion through NSW Treasury's websites or other mechanisms
- details of personal, medical, health, financial, and other personal ascertainable information about the personal circumstances of NSW Treasury staff
- details of correspondence, which can include sensitive personal information about correspondents or NSW Treasury staff on matters such as an individual's ethnicity, religion, health conditions, or sexuality
- copies of replies to correspondence
- records of to whom correspondence has been referred.

Correspondence records (including originating correspondence and responses) are stored in NSW Treasury's information systems in accordance with NSW Treasury's Record Management Framework. Certain correspondence records (for example, correspondence received by the Minister or Members of Parliament concerning issues of major significance) are required to be retained indefinitely as State Archives under the *State Records Act 1998*.

## 11 Client/Customer records

Any online correspondence received via the Feedback Assist platform will be stored on the Salesforce platform, which is under the control and custody of the Department of Customer Service (DCS). Where such personal information comes into NSW Treasury's possession, it will be used only to respond to queries and/or to onforward to the correct agency that NSW Treasury believes is better placed to respond.

## 12 Information collected from public submissions

NSW Treasury may conduct reviews requesting public submissions from members of the public. The reviews may contain personal information about individuals such as:

- address, and contact details
- personal and business circumstances (where it concerns a sole trader or individual that can be readily ascertained)
- ethnicity, religion, health conditions, or sexuality
- third party information
- information that may meet the definitions under the *Children and Young Persons (Care and Protection) Act 1998*.

This personal information will only be used for the purpose of undertaking and completing a review relating to its terms of reference. Once the review has been completed, a copy will be placed on NSW Treasury's website as an authorised proactive release of government information (section 7 of the GIPA Act). No personal information will be released except with the express written consent of the affected persons.

When inviting public submissions, NSW Treasury should set clear expectations about what information will and will not be published. Typically:

- all submissions received by NSW Treasury will be published via NSW Treasury website
- personal information will be redacted unless express written consent is provided
- individuals and organisations may ask to make confidential submissions that are not published.



52 Martin Place  
Sydney NSW 2000

GPO Box 5469  
Sydney NSW 2001

W: [treasury.nsw.gov.au](https://treasury.nsw.gov.au)

This publication is protected by copyright. With the exception of (a) any coat of arms, logo, trade mark or other branding; (b) any third party intellectual property; and (c) personal information such as photographs of people, this publication is licensed under the Creative Commons Attribution 3.0 Australia Licence.

The licence terms are available at the Creative Commons website at:  
[creativecommons.org/licenses/by/3.0/au/legalcode](https://creativecommons.org/licenses/by/3.0/au/legalcode)

NSW Treasury requires that it be attributed as creator of the licensed material in the following manner: © State of New South Wales (NSW Treasury), (2023).

