NSW Treasury

Privacy Management Plan and Guidelines (PMP)

TIPP 5.19

14 April 2024

NSW GOVERNMENT

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.

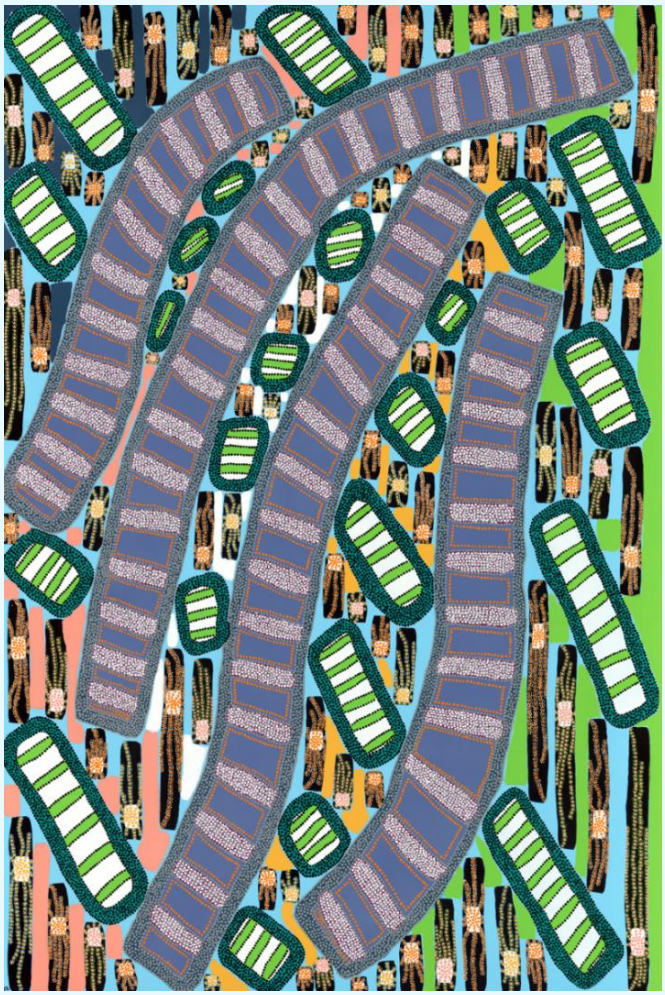
We pay respect to Elders past and present and commit to respecting the lands we walk on, and the communities we walk with.

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: 2.0
Original issue date	17 November 2023
Version 2 issue date	14 April 2024
To be reviewed	April 2026
Related instrument(s)	Data Breach (Privacy) Policy TIPP 5.20 Data Breach (Privacy) Response Plan and Procedure TIPP 5.20a (Internal Document)
Document approver	Secretary, NSW Treasury

Version History	
Version 1	Original. Developed for new s33 PPIP Act requirements
Version 2	Updated. Improvements made after review and internal stakeholder consultation and updated for digital reporting and data breach processes.

Contact details	
Position:	Special Counsel
Division:	Office of General Counsel
Branch:	Governance, Ethics, and Integrity
Email:	governance@treasury.nsw.gov.au

Contents

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

14 April 2024

Note

General inquiries concerning this document should be initially directed to:

Office of General Counsel, NSW Treasury: governance@treasury.nsw.gov.au.

This publication can be accessed from the Treasury's website 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.

NSW Treasury's 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 5.20a Data Breach (Privacy) Response Plan and Procedure (Internal document)
- TIPP 5.20 Data Breach (Privacy) Policy (Public facing document)

1.2 Policy scope, review, dissemination

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

It outlines NSW Treasury's practices to ensure compliance with the requirements of the PPIP and HRIP Acts and other legislation as applicable.

The PMP and Data Breach policies (see above) have been created through stakeholder consultation across Treasury to ensure compliance is embraced and achieved.

These privacy policies will be reviewed regularly in accordance with legislative changes and NSW Treasury requirements. Next review date is stated in the Version table (unless required earlier).

The PMP is available on Treasury's external and Intranet sites. NSW Treasury privacy policies and practices are also promoted regularly through the following:

- New Starter mandatory privacy training package/s
- Annual mandatory staff training in privacy
- Regular privacy promotion staff emails and Treasury messages
- Privacy Champions promotion and engagement roles
- Active participation in annual Privacy Awareness Weeks
- Mandatory digital Privacy Impact Assessments (PIAs) for all work undertaken involving personal or health information
- Mandatory Privacy Data Breach reporting and consideration of privacy impacts in all incidents.

NSW Treasury will also provide the NSW Privacy Commissioner with a copy of this Privacy Management Plan as soon as practicable after it is prepared and whenever the plan is amended.

2 Privacy Obligations and Risk

2.1 What types of information concern privacy?

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.

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 F:.

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 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		
Collection	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.
Storage	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.
Access	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.
Use	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.
Disclosure	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 on how the HPPs apply to NSW Treasury:

12 Health Privacy Principles		
Collection	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.
Storage	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.
Access	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.
Use	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: (a) the person has consented to its use for another purpose (b) it is being used for a purpose directly related to the purpose it was collected for (c) we believe that there is a serious threat to health or welfare (d) it is for the management of health services, training, research or to find a missing person (e) it is for law enforcement or investigative purposes.
Disclosure	11.	Restricted – We only disclose health information for the purpose it was collected for unless: (a) the person has consented to its disclosure for another purpose (b) it is being disclosed for a purpose directly related to the purpose it was collected for (c) we believe that there is a serious threat to health or welfare (d) it is for the management of health services, training, research or to find a missing person (e) it is for law enforcement or investigative purposes.
Other	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 Privacy Impact Assessments (PIAs)

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 a PIA is to assess and consider any privacy issues before a project, review, or other policy deliverables are undertaken. A PIA can be a helpful defence if something does go wrong and help prevent problems in the first place by anticipating potential risks. PIAs are also important tools (especially if published) to help build public trust and confidence in how NSW Treasury handles personal information.

A PIA digital tool has been developed to assist this process. Links are available internally on the NSW Treasury Intranet.

Examples of when to use the PIA tool could include (but are 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 taken at a stakeholder event
- contact/personal details collected and kept for mailouts, invitations, submissions etc.
- changes to projects
- updates to databases
- historical data that hasn't had a PIA completed before.

Treasury's PIA tool is a 2 stage process. It consists of 2 form submissions. Templates of these forms are available at Appendix A: and Appendix B:**Error! Reference source not found.** and Treasury has digitalised this process.

3.1 Form 1 Rapid Privacy Threshold Assessment (RPTA)

The first step using the digital PIA tool is to complete a Rapid Privacy Threshold Assessment (RPTA). The questions assess if personal information is involved and/or if privacy is a factor to be considered.

If you are unsure about privacy requirements for a specific project, the Rapid Privacy Threshold Assessment (RPTA) can help you decide if the information that you have or plan to collect has privacy implications.

A PIA should be completed for existing databases of personal/contact information as well as new collections of personal information.

A copy of the RPTA form can be found at Appendix A.

If privacy issues **are** involved, you will be required to complete a more detailed Privacy Impact Assessment (PIA) including a Risk Table.

3.2 Form 2 Privacy Impact Assessment (PIA)

After completing the above RPTA, if privacy is involved you will be required to continue to complete a detailed Privacy Impact Assessment (PIA), including a Risk Table, within Treasury's digital PIA tool.

The detailed PIA enables you to assess and consider any privacy issues before a project, review, or other policy deliverables are undertaken, or changes or updates are made to processes or existing information is being assessed or reassessed.
For a copy of the PIA template, see Appendix B.

The 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 11/12 or above.

Prior to approval it must be endorsed by the line area Privacy Champion, Privacy Officer, or OGC Support lawyer.

Once it has been approved, a copy will be provided electronically to the line area.

Privacy tips:

- The PIA digital forms should be completed for all projects and bodies of work. It is the responsibility of the project/work owner to ensure privacy is considered and any risks reduced. Should an exemption to this requirement be desired, an application would need to be made to the Secretary as to the reasons why the exemption is sought.
- When planning to collect personal/health/sensitive information, 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.
- Existing information we hold must also now be assessed in the light of privacy risks and the privacy principles need to be applied to all existing projects, database, and contact information.
- 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 sensitive, 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 GPDR. This includes if you are collecting information about and tracking web-based behaviour, where that behaviour is coming from the EU.

3.3 What to consider in completing a PIA

Collection

When collecting personal information, NSW Treasury should issue a Privacy Notice that explains:

- 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:.

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

Use and disclosure

You must always consider, how you are going to use the information, and 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?

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 access 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 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 access 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 governance@treasury.nsw.gov.au.

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

4 Roles and responsibilities of NSW Treasury employees

4.1 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 staff privacy awareness
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).

To contact the Privacy Coordinator please email governance@treasury.nsw.gov.au

4.2 Privacy Officers and Champions

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

1. **Providing Advice and endorsement**
    a. Providing advice to their groups about handling personal information, responding to general enquiries from their teams.
    b. Support, assess and endorse PIAs and where necessary escalate to the Privacy Coordinator for any complex PIAs that raise 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 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 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 (PSSE) Band 1 or above who have been nominated by their Deputy Secretary to undertake this function.

Privacy Officers are all OGC legal officers at Clerk Grade 5/6 and above, all staff reporting to the Lead Associate Director GE&I, the Associate Director Information Access, and all members reporting to the Director, Risk, Compliance and Audit at clerk grade 9/10 and above.

4.3 Treasury staff

All Treasury staff are required to follow this Privacy Management Plan and all the requirements stated.

Treasury staff are expected to:

1. complete privacy mandatory training
2. assess all work with respect to privacy implications and complete the PIA tool as required
3. report privacy data breaches
4. follow all record keeping policies and practices
5. follow the highest standards of practice in relation to protecting personal information.

Staff should contact their Privacy Champion, Privacy Officer, or the Privacy Coordinator, should they require further assistance.

5 Privacy Data Breaches

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 report a privacy data breach

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

How to make a report

NSW Treasury has developed a digital reporting tool for ease of reporting and to encourage and assist staff to report efficiently and swiftly any suspected privacy data breach. The digital form is available on the intranet.

For steps to be followed and practical guidance in a data breach, the Data Breach (Privacy) Response Plan and Procedure TIPP 5.20a is available for access to NSW Treasury employees. It includes specific security controls and operational protocols and outlines in detail Treasury's response plan and how Treasury meets its reporting and response obligations.

5.1 Mandatory Notification of Data Breach (MNDB) Scheme

The Data Breach (Privacy) Policy TIPP 5.20 provides the framework as to how Treasury will meet its obligations under Part 6A of the PPIP Act *Mandatory notification of data breaches.* The Response Plan and Procedure TIPP 5.20a details the steps taken within Treasury in responding to a data breach.

In summary, eligible data breaches must follow the requirements of Part 6A including reporting and notification requirements.

Eligible data breaches are where there is unauthorised access or disclosure of personal information which would likely result in serious harm.

The digital reporting tool Treasury has developed, enables speedy acknowledgement of any suspected privacy data breach and ensures NSW Treasury meets all its obligations under the Scheme.

Please see The Data Breach (Privacy) Response Plan and Procedure TIPP 5.20a for details.

5.2 Privacy complaints

When to make a complaint

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).

5.3 Review processes

Internal Reviews

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 Act sand 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 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 E:

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:

- 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.

Records 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 Reviews

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).

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.

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 A: Rapid Privacy Threshold Assessment Tool

The RPTA is the first step in the PIA tool. The PIA tool is available for staff internally on the Privacy tab of the Intranet home page. The RPTA template is available there as well and is shown below. Once submitted, if the answer is yes, you will be directed to complete a more detailed Privacy Impact Assessment (PIA) (Appendix B).

Privacy Impact Assessment (PIA)

(Name of Project here)

[Click here to enter a Date]

Prepared by:	
Position:	
Email:	
Phone:	

Scope

This is a Rapid Privacy Threshold Assessment (RPTA). It is used to initially determine if a body of work, database, or new project has any privacy implications. If privacy issues are involved a detailed Privacy Impact Assessment (PIA) must also be completed.

Applicable 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"**

Stakeholders Consulted

Stakeholder	Internal/ External	Scope of Consultation

Project Outline

#	Question	Answer
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 RPTA)	
6	Project manager	
7	Director	
8	Executive Director	

Step 1- Rapid Privacy Threshold Assessment (RPTA)

#	Question	Answer – YES / NO / UNSURE
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?	
#	**Question**	**Answer**
14	Describe the information that is being collected and how it is going to be presented?	Detailed description

Instructions

If you answered YES to any of the above, please complete a detailed Privacy Impact Assessment (PIA) and attach to the above before forwarding to your Privacy Champion.

If you answered NO or UNSURE to any of the above, please forward this PIA (with only Step 1 Rapid Privacy Threshold Assessment (RPTA)) to your Privacy Champion, Privacy Officer (OGC lawyer) or the Governance, Ethics and Integrity team (GEI).

Privacy Champions can be found here on the Intranet

GEI can be contacted at governance@treasury.nsw.gov.au

Endorsement and Approvals

These endorsements and approvals are for an RPTA with NO identifiable privacy impacts.

Privacy Champion

Having reviewed the responses above, I am satisfied that a full Privacy Impact Assessment is not required.

Name:			
Position:			
Signed:		Date:	

Comments:

Director Approval

Name:			
Position:			
Approved / Not Approved			
Signed:		Date:	

Comments:

Executive Director Approval

Name:			
Position:			
Approved / Not Approved			
Signed:		Date:	

Comments:

Appendix B: Full Privacy Impact Assessment (PIA)

This mandatory PIA is used to assess and mitigate privacy impacts when:
1. required by the outcome of your Rapid Privacy Threshold Assessment (RPTA) (Appendix A**Error! Reference source not found.**), or
2. requested to do so by the Privacy Coordinator, Privacy Champion or Privacy Officers, or
3. if you and your team collect, use, store and/or disclose personal or health information.

The PIA digital tool will require you to complete Step 1 – RPTA (Appendix A) then direct you to continue to complete the more detailed Step 2 - PIA (Appendix B) if required.

Step 2- Privacy Impact Analysis (full PIA)

(Continued from RPTA Appendix A Step 1 which must be completed first)

Information Involved

#	Question	Answer
15	What types of personal, health and sensitive information are being collected, stored, used or disclosed in the project that may identify individuals?	
16	Provide reasons why you are capturing the information selected above.	

Collection

#	Question	Answer
17	Is the personal and/or health information being collected directly from the individual?	
18	Will the program assign a unique identifier to an individual when personal information is being collected?	(e.g. survey response number)
19	Has a privacy notice been prepared to inform the individual of the method and primary purpose for the collection, storage, use or disclosure of their personal and/or health information with a copy of NSW Treasury's Privacy Management Plan and Guidelines?	
20	Briefly describe the flow of information, systems used, and parties involved in the project.	

Use and Disclosure

#	Question	Answer
21	Will the personal information (or sensitive information) be used or disclosed ONLY for the main or primary purpose for which it was collected?	
22	If not, explain how individuals will be given notice of the additional use(s) of their personal information, or why notice of additional use(s) will not be provided.	
23	Will any personal information collected for this project/program be de-identified?	
24	Will any data matching occur as part of this program? This includes matching datasets within the program or matching to other datasets external to the program?	

Storage and Security

#	Question	Answer
25	Where and how will personal information be stored?	
26	Describe how you will ensure the ongoing accuracy, completeness, and currency of the personal information used in this program?	
28	Are you using Treasury IT approved systems to collect, store, use, and disclose personal information?	
29	Are there security measures in place (existing or intended) to protect the personal information collected and used for this project/program? Please provide details.	

30	Where information is stored internally, are there exceptions required to the standard Treasury disposal process?	
31	If applicable, what will happen to personal information held by third parties? Please provide names of 3rd parties.	

Access, Amendment and Other Requirements

#	Question	Answer
32	Who will have access to the personal information?	
33	How can individuals request access to, or correct their personal information?	
34	Will any personal information be shared outside of Treasury?	
35	Outside of Treasury Approved IT systems, will you be transferring any personal information outside Australia?	
36	Who can individuals complain to if they have concerns about the handling of their personal information?	
37	What actions are in place for staff to ensure the appropriate collection and handling of the personal information collected for this program? (e.g., staff training)	

Information Workflow and Diagram Risk Assessment

#	Question	Answer
38	Please describe, or use a diagram/table, to show the flow of information in this project, indicating the systems used and parties involved, and methods of transferring the information (if applicable). Where possible, indicate the types of information	

	that flow between stages or parts of the program, and between different parties.	
38.1	Please complete the following Risk Table	See below

RISK TABLE

Once you have considered all the Information Protection Principles (IPPs) – Collection, Use and Disclosure, Storage and Security, Access, Amendment and Other Requirements, in the Information Flow Diagram of the PIA, in addition to explaining how the information travels through the project's lifecycle, **complete the table below**, listing all the risks that were identified during the assessment stage.

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

Stakeholder Consultation

#	Question	Answer
39	Key internal stakeholders	
40	Key external stakeholders	
41	Have the project manager and key stakeholders been consulted in the preparation of this PIA for the project?	
41.1	Please summarise the outcome of the stakeholder consultation	
43	Will this Privacy Impact Assessment be published?	
44	How will the program be evaluated against its objectives?	
45	Please expand on any other broader privacy considerations associated with this program that have not been covered in this assessment:	
46	Does the project/program comply with NSW Treasury's other information handling or information management policies?	

Submit PIA

#	Question	Answer
47	Please confirm that the PIA is ready to be submitted for sign-off	
48	Who will sign off on this PIA?	

Endorsement and Approvals

Privacy Champion

Having reviewed the responses above, I endorse this PIA.

Name:			
Position:			
Signed:		Date:	

Comments:

Director Approval

Name:			
Position:			
Approved / Not Approved			
Signed:		Date:	

Comments:

Executive Director Approval (Only if a PIA is not required)

Name:			
Position:			
Approved / Not Approved			
Signed:		Date:	

Comments:

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

The following ***Privacy Notice Template*** 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.**

Privacy Notice Template

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.

[*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: Making a privacy complaint (for internal review)

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

☐ S53 of the ***Privacy and Personal Information Protection Act 1998*** (the PPIP Act)
☐ S21 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.

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? ☐ yes ☐ no ☐ 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)* ☐ collection of my personal or health information ☐ security or storage of my personal or health information ☐ refusal to let me access or find out about my own personal or health information ☐ accuracy of my own personal or health information ☐ use of my personal or health information ☐ disclosure of my personal or health information ☐ other ☐ 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	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: Click or tap here to enter text.
10	What effect did the conduct have on you? Click or tap here to enter text.
11	What effect might the conduct have on you in the future? Click or tap here to enter text.
12	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.)* Click or tap here to enter text.
13	I understand that this form will be used by NSW Treasury to process my request for an Internal Review. 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 the review. I would prefer the Privacy Commissioner to have: ☐ a copy of this application form, or ☐ just the information provided at questions 5-12.

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

Alternatively, you can email this form to: governance@treasury.nsw.gov.au

Please keep a copy for your own records

Appendix E: Draft letter to the NSW Privacy Commissioner

Letter template 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 F: Types of personal and health information held by NSW Treasury

Employee records

NSW Treasury and contracted service providers (such as GovConnect, Contractor Central, myCareer,) 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, 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.

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.

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.

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.

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.

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.

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.

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*.

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.

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

NSW GOVERNMENT