Privacy Management Plan

Sydney Metro

Version 4 | November 2023*

Review Date: November 2024

* Amended April 2024 to include link to March 2024 Transport Code of Conduct

Contents

1 Introduction

Sydney Metro takes the privacy of our staff and the people of NSW seriously, and we will protect the personal and health information we collect and hold in accordance with *Privacy and Personal Information Protection Act 1998* (**PPIP Act**), the *Health Records and Information Privacy Act 2002* (**HRIP Act**) and this Privacy Management Plan (**Plan**).

We aim to create a strong culture of privacy compliance and best practice by:

- applying a 'privacy by design' approach to new projects, including undertaking privacy impact assessments where appropriate;
- ensuring the public are well informed about what personal information Sydney Metro collects and how it is handled;
- promoting staff awareness of Sydney Metro's privacy obligations through targeted campaigns, training and intranet resources.

In the event of a data breach, Sydney Metro's Data Breach Policy (see section 7) and Privacy Data Breach Response Procedure set out the requirements for managing and responding to the breach.

The roles and responsibilities of staff are contained in Appendix D.

1.1 Purpose of this Privacy Management Plan

The Plan is an important tool in explaining:

- how Sydney Metro upholds and respects the privacy of our customers, staff and others about whom we hold personal information;
- who you should contact with questions about the information collected and held by Sydney Metro;
- how to access and amend your personal information; and
- what to do if you think Sydney Metro may have breached its privacy obligations under PPIP Act or HRIP Act.

In addition, this Plan acts as a reference tool for Sydney Metro staff to explain how we can best meet our privacy obligations under the PPIP and HRIP Acts. As public sector officials, Sydney Metro staff are required to comply with the PPIP and HRIP Acts and the *Security of Critical Infrastructure Act 2018* (which has separate reporting obligations in relation to critical infrastructure). This Plan is intended to assist staff to understand and comply with their obligations under the legislation and also addresses the requirements under section 33 of the PPIP Act to have a privacy management plan.

The PPIP Act and HRIP Act contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information. For example, there are offences relating to:

- Corrupt disclosure and use of personal information by public sector officials; and
- Offering to supply personal or health information that has been disclosed unlawfully.

Sydney Metro's staff are regularly reminded of their responsibilities under the PPIP Act and HRIP Act and these obligations are reinforced in our Code of Conduct and through initiatives outlined in Part 4 of this Plan.

Where possible Sydney Metro enables individuals to interact with it anonymously, for example, when providing feedback.

1.2 About us

Sydney Metro was established on 1 July 2018 under the *Transport Administration Act 1988* (NSW) (**TAA**) as a NSW Government agency with the principal objectives of delivering safe and reliable metro passenger services in an efficient, effective and financially responsible manner, and to facilitate and carry out the orderly and efficient development of land in the locality of metro stations, depots and stabling yards, and proposed metro stations, depots and stabling yards.

As a NSW Government agency, Sydney Metro is required under section 33 of the PPIP Act to have a privacy management plan.

1.3 Contact us

For further information about this Plan or any other concerns about your privacy, including:

- how Sydney Metro manages personal and health information
- requests for access to and amendment of personal or health information
- guidance on broad privacy issues and compliance
- requests to conduct internal reviews about possible breaches of the PPIP Act and HRIP Act

you may contact the Sydney Metro Privacy Officer via TfNSW:

Post: Legal, Privacy & Information Access Branch
Transport for NSW
PO Box K659
Haymarket NSW 1240

Email: privacy@transport.nsw.gov.au

If Sydney Metro staff feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Sydney Metro legal team.

2 Personal and health information held by Sydney Metro

Sydney Metro does not maintain any public registers for the purposes of the PPIP Act or HRIP Act.

2.1 Sydney Metro information holdings

Examples of personal and health information collected and held by Sydney Metro in the exercise of its functions include:

Staff and recruitment

During the recruitment process and throughout employment, information (including personal and/or health information) is collected from applicants and staff for various reasons such as leave management, workplace health and safety and to help Sydney Metro operate with transparency and integrity.

Successful applicants are invited to fill out various forms in order to commence employment at Sydney Metro which invite people to provide sensitive personal information such as racial and cultural information in order to collect data about the wider NSW public sector. Disclosing this information is voluntary.

These forms are sent to the Talent and Payroll teams to be used for employment purposes such as setting up personnel files. This information is kept securely in an enterprise database.

- Applicant's contact details
- Employee's bank details and tax file number
- Lists of the direct contact details, including telephone numbers and email addresses for departmental staff
- Flex sheets/Attendance records
- Travel and expense reimbursement
- Salary sacrifice paperwork
- Superannuation details
- Leave details (including medical certificates)
- Payslips
- Higher duties applications
- Emergency contact details (including telephone number, postal and email address)
- Discipline and conduct information
- Performance management records
- Records of gender, ethnicity and disability of employees for equal employment opportunity reporting purposes
- Background information (such as criminal history, ethnic background, disability)
- Medical conditions and illnesses
- Next of kin and contact details
- Education
- Family and care arrangements
- Secondary employment
- Conflicts of interest

	• Financial information for payroll purposes • Employment history Note: Job applications (cover letter, resume and selection criteria responses) are information about an individual's suitability for employment as a public sector official and so this information is not personal information. Sydney Metro still treats this information confidentially.
Rail Industry Worker information	• Personal Information collected via the Rail Industry Worker cardholder scheme • Name • Contact information • Qualifications • Visa status • Health information
Injury and Claims Management	• Health records (including medical certificates, reports and files and fitness for duty assessments) • Drug and alcohol records • Return to work paperwork • Workers Compensation records • Injury management paperwork • Occupational Health and Safety records
Workplace Conduct and Investigations	• Personal information of employees involved in investigations • Name, addresses, contact details and other relevant information of witnesses and/or complainants (members of the public - non employees) • Photographs • CCTV footage • Statements • Investigation reports which may include the above information
Community and stakeholder engagement / communications	• Contact details for community and industry stakeholders Contact details for government agency CEOs, members of inter-departmental working groups and the like, members of government boards and advisory committees • Contact details for stakeholders and

	local residents participating in community consultations and the organisations they represent • Contact details and contractual information for performers hired for public events • Contact details for people who enter competitions • Contact details for volunteers who assist at public events, as well as (where relevant) their dietary requirements, any mobility restrictions, shirt size or drivers licence information • Personal information in emails and other correspondence e.g. public-facing Outlook mailboxes • Financial information (such as credit card information – for example, for the purpose of GIPA application fees)
Various Sydney Metro occasionally holds community events or participates in events held by other agencies or organisations. During these events, Sydney Metro may collect general information such as the number of visitors to a stall, questions visitors asked, what resources were provided and general demographic information such as gender.	• Customer surveys may capture personal information • Names and contact details of contractors • Contact details of people who have written to or emailed the Minister, with details of the nature of their correspondence. • Statements and opinions (general enquiries, consultation, feedback and complaints) • Audio recordings (where incoming telephone conversations are recorded for quality and assurance purposes) and interviews • Photographs and CCTV footage
Website publishing, photography and media Sydney Metro owns and maintains the website sydneymetro.info Sydney Metro does not publish personal or health information on the website without permission.	• Website data • Photos or filming of events (Sydney Metro will seek permission from people before taking photos or filming events and advise them how Sydney Metro will manage the images and what they will be used for. Those who agree can be asked to sign a consent form).
Learning and Development	• Information collected as a result of conducting training as a Registered Training Operator, including details such as:

	• Student Name • Contact Information • Enrolment and Result Information

Sydney Metro Legal Corporate must be consulted regarding proposals to share or disclose sets of personal information held by Sydney Metro.

2.2 Significant Information Systems

Significant information systems operated by Sydney Metro include:

SAP Corporate	HR and finance systems
iCentral	Document management system
InEight Document	Project management software
Primavera P6	Project management software
Image Library	Online image library to store and catalogue photos, images, videos, sound and logos
Rail Industry Worker System (MTA and Pegasus)	System to administer and manage the national safety and competency management program for Australian rail industry workers
INX	Incident management database

3 How Sydney Metro manages personal and health information

This section describes how Sydney Metro uses, discloses and stores personal and health information in alignment with its functions and activities, and with standards which Sydney Metro is expected to follow when dealing with personal information and health information.

Key definitions, including a description of what is and is not personal or health information are located at Part 7.

3.1 Collection of personal and health information – key principles

*PPIP Act **Sections 8-11**, HRIP Act **HPPs 1-4***

Collection must be:

- *for a lawful purpose;*
- *directly from an individual;*
- *meet specific requirements for notice; and*
- *relevant, not excessive, accurate and not intrusive.*

We won't ask for personal information (especially sensitive personal information) or health information unless we need it to perform our functions. This makes it easier to comply with our other obligations. For example, if we need to know an individual's age to provide age-appropriate services, we will ask for their age or their year of birth, not their exact date of birth.

We will take reasonable steps to ensure that the personal and health information we collect is relevant, accurate, up-to-date, complete and not unreasonably intrusive or excessive.

We will only collect personal and health information about a person from a third party where:

- it is lawful to do so, or the individual has authorised collection of the information from someone else; or
- the individual is under 16 years of age – in which case we may collect information from the individual's parent or guardian; or
- it would be unreasonable or impracticable to collect information directly from the individual.

We will take reasonable steps to ensure that information collected is not unreasonably intrusive or excessive, and is relevant, accurate, up-to-date and complete before using it.

Usually, we rely on the person providing the information to confirm its accuracy when it is provided. Sometimes we will independently verify the information provided.

Where reasonable to do so, we will notify members of the public that their information is being collected via a 'privacy notice', which will be included on an application form, web page, recorded message or in a verbal notice at the time the personal or health information is collected, or as soon as practicable afterwards.

The information generally contained in a privacy notice will include:

- the fact that information is being collected
- the reason(s) why the information is being collected
- what the information will be used for
- where the personal information will be stored
- an ‘opt out’ for people who do not wish for their information to be collected.

3.2 Use and disclosure of personal and health information – key principles

PPIP Act **Sections 16-19**, *HRIP Act* **HPPs 9-11 & 14**

An agency *must:*

- *Check the information before using it to make sure it is relevant, up to date, complete and not misleading;*
- *Not use information for a purpose other than the collection purpose except in limited circumstances; and*
- *Not disclose information for a purpose other than the collection purpose except in limited circumstances.*

We will only use personal and health information for:

- the purpose, or a purpose directly related to the purpose, for which it was collected;
- another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health of any person;
- another purpose for which the individual has consented; or
- another purpose where permitted by law.

Some examples of where the law permits us to use personal or health information for another (secondary) purpose include:

- quality assurance activities such as monitoring, evaluating and auditing;
- work health and safety laws require that we use information to ensure the safety of our employees; or
- unsatisfactory professional conduct or breach of discipline.

We may use or disclose insights or trends derived from aggregated personal information (data). In this case Sydney Metro will ensure the removal of identifiers of personal information so that the information is not about an identifiable person.

When we disclose information, it means that we give it to a third party outside Sydney Metro. We will only disclose personal information (including to third party agencies) if:

- the disclosure is directly related to the purpose for which the information was collected; or
- the individual has been made aware in the relevant privacy notice that information of the kind in question is usually disclosed to the recipient; or
- we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health; or
- where the disclosure is otherwise authorised by law.

3.4.1 Disclosure between Transport agencies.

NSW Government departments, agencies and organisations are arranged into nine

groups, called clusters. TfNSW, Sydney Trains, NSW TrainLink and Sydney Metro are executive agencies related to the Department of Transport, and therefore within the Transport cluster. Clusters have no legal effect for privacy purposes. However, they must comply with the applicable privacy principles. Where Transport agencies use personal or health information internally, this will constitute a “use” for privacy purposes. Where Transport agencies provide information to another person or body, including another agency within the Transport cluster, this will constitute a “disclosure” for privacy purposes.

Transport cluster employees should be aware that there is no special provision for giving personal or health information to other agencies within the Transport cluster. Care should be taken to ensure that any such disclosure complies with applicable privacy requirements. If you are not sure, check with the Legal privacy team.

Transport may disclose personal or health information to a Transport cluster agency in circumstances including:

- while seeking legal advice, where legal services are provided by Transport
- to enable inquiries to be referred between the agencies concerned
- under a delegation to enable the Transport agency to exercise employee functions, or
- where the disclosure is reasonably necessary for law enforcement purposes, including the investigation of suspected fraud.

However, prior to doing so the agency will either: de-identify all personal information before seeking advice from another agency: or obtain prior consent from the individual who the information is about before disclosure; or rely on any available exemptions.

Transport agencies may share de-identified data between themselves for research and analysis.

Our collection notice will tell you when we disclose your personal information. We have formal arrangements in place which govern the way we share personal and health information with other government agencies. In each case, disclosure is either for the purpose for which the information was collected or is made under lawful authorisation.

The HPPs also contain other reasons the Transport agencies may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual or another person, in order to help find a missing person, or for compassionate reasons.

When we disclose information to a party or agency in another jurisdiction we seek consent before doing so, where possible.

3.4.2 Sensitive information

PPIP Act **Section 19**, *HRIP Act* **HPP 14**

An agency must:

- *Comply with special restrictions on disclosing or transferring sensitive information outside NSW.*

We recognise that additional protection must be given to sensitive personal information (relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities). We can generally only disclose sensitive personal information when the individual has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health.

In the case of health information, we can disclose health information for the primary collection purpose or when:

- the disclosure is directly related to the purpose for which it was collected and the individual would reasonably expect us to disclose the information for that purpose;
- the individual has consented to the disclosure; or
- the disclosure is necessary to prevent or lessen a serious and imminent threat to life, health or safety.

Circumstances in which we may disclose personal and health information include when we are managing investigations, complaints or claims. In many cases where we use personal or health information we anonymise it first. We do not disclose health or personal information to individuals or bodies outside of NSW.

3.3 Retention and Security

PPIP Act **Section 12**, *HRIP Act* **HPP 5**

An agency *must:*

- *Keep information only for as long as necessary for its lawful purposes for use;*
- *Dispose of the information appropriately;*
- *Protect the information through appropriate safeguards; and*
- *Do everything reasonably within its power to protect the information when the information is given to another person to provide a service to the agency.*

Sydney Metro stores information in a variety of ways, including on Sydney Metro databases, cloud storage by third parties and in various physical locations.

Some of the security measures taken by Sydney Metro include:

- restricting access to all IT systems and databases to ensure that only authorised users with a clear business need can access them;
- use of strong passwords for computer access and a mandatory requirement that all staff change computer access passwords on a regular basis;
- use of print on demand (secure printing);
- implementing and maintaining security software across all network components in arrangements for data transmissions (including encryption and password protection where appropriate), backup and storage;
- providing staff with access to secure storage spaces near workstations to secure documents and devices;
- physically securing sensitive and confidential information in locked rooms;
- implementing and observing a clean desk policy;
- physically separating business areas from other business areas who deal with large amounts of personal and health information on a day-to-day basis into secure areas of the building;
- maintaining and continually improving transport information security management systems that comply with ISO/IEC 27001:2013 standard;
- aligning with our obligations under the NSW Government *Information Management Framework* and *Cyber Security Policy 2019;*
- adopting best practice in electronic and paper records management and complying with our obligations under the *State Records Act 1998* (NSW);
- keeping information for only as long as necessary and disposing of information securely;
- where it is necessary for information to be transferred to a third party provider for the purposes of providing us with a service, we develop and execute contract terms that prevent unauthorised use or disclosure of information that we hold;
- providing mandatory information security awareness training to Sydney Metro staff;
- monitoring of usage through access logs and regular audits;
- training on data protection and use;
- monitoring of data feeds and transfers;
- logging of where personal information is through data management tooling.

Sydney Metro engages in continuous improvement of each of its existing security measures by reviewing and enhancing the measures in place to protect all personal information held by Sydney Metro with particular focus on critical systems.

3.4 Exemptions from the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs)

3.4.3 Exemptions from IPPs

PPIP Act sections 22-28 *relating to law enforcement and related matters; ASIO; investigative agencies; lawful authorisation; where non-compliance benefits an individual; specific exemptions for statutory agencies; information exchanges between public sector agencies; research; credit* information*; and other exemptions.*

The PPIP Act contains exemptions that may allow Sydney Metro to not comply with IPPs in certain situations. For example, we may not be required to comply with the following IPPs in some circumstances:

- Direct collection (section 9 (IPP 2) of the PPIP Act);
- Notice (section 10 (IPP 3) of the PPIP Act);
- Access and transparency (sections 13 to 15 (IPPs 6 to 8) of the PPIP Act); or
- Use and disclosure (sections 17 to 19 (IPPs 10 to 12) of the PPIP Act).

We do not use the other exemptions on a regular basis as they are not usually relevant to our work or functions. However, if an exemption was to be used, we aim to be clear about the reasons for using it.

3.4.4 Exemptions from HPPs

Exemptions are located mainly in Schedule 1 of the HRIP Act and may allow Sydney Metro to not comply with HPPs in certain situations.

For example, we are not required to comply with the HPPs in clauses 4 to 8 and 10 if we are lawfully authorised, required, or permitted not to comply with them.

We do not use the other exemptions on a regular basis as they are not usually relevant to our work. However, if an exemption were used, we aim to be clear about the reasons for using it.

4 How to access and revise your information

PPIP Act **Section 13-15**, *HRIP Act* **HPPs 6-8**

An agency *must:*

- *Take reasonable steps to enable any person to ascertain details of the information the agency holds about them;*
- *When requested, provide individuals with access to their information without excessive delay or expense; and*
- *Make appropriate amendments or make notations to ensure the information remains accurate, relevant, up to date, complete and not misleading.*

Everyone has the right to access the personal and/or health information Sydney Metro holds about them. They also have the right to change their own personal and/or health information Sydney Metro holds, for example, updating their contact details. However, if Sydney Metro thinks in the circumstances that it is not appropriate to amend the information then you can request a statement about the requested changes be attached to the information.

Sydney Metro is required to provide you with access to the personal and/or health information it holds about you and allow you to amend this information without expense or excessive delay.

Sydney Metro encourages you to keep your personal and/or health information up-to-date and accurate, particularly your personal and next of kin contact details (in case of an emergency). It is also your responsibility to inform us if you wish to change your bank account details or payment details.

If Sydney Metro considers that it is not appropriate to amend particular personal and/or health information, then you may provide a statement about the amendments that you sought to make in a manner that is capable of being read with your original personal and/or health information.

This section explains how to request access to your own personal and/or health information via an informal or formal application, and what to do if you need to amend your personal and/or health information held by Sydney Metro.

4.1 Members of the public

Often we rely on the person providing the information to confirm its accuracy, for example, stakeholder feedback on a project. Sometimes we will independently verify the information.

In some cases, you may be able to access and request amendments to your own personal and/or health information by contacting the business unit involved and making an informal request.

If you do not know which business unit within Sydney Metro to contact about your request or your request has been denied, please fill out and submit an Application Form – Access or email sydneymetro.privacy@transport.nsw.gov.au.

4.2 Employees

Employees can access their personnel files by either making a request to Transport Shared Services (**TSS**) or by contacting HR Advisory on 1800 618 445 or at tfnswhr@transport.nsw.gov.au

Files about disciplinary matters and grievances are confidential and access is generally provided only to the staff member to whom the file relates. Generally, staff may inspect files under supervision and will also be able to take photocopies of material on their file.

4.3 Accessing or amending other people's information

The PPIP Act and the HRIP Act give people the right to access their own information; the Acts generally do not give people the right to access someone else's information.

However, section 26 of the PPIP Act allows an individual to give consent to Sydney Metro to disclose their personal information to someone else who would not normally have access to it.

Similarly, under sections 7 and 8 of the HRIP Act, an 'authorised representative' can act on behalf of someone else. The HPPs also contain information regarding other reasons Sydney Metro may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual or another person, in order to help find a missing person, or for compassionate reasons.

If none of these circumstances are relevant, a third party can consider making an application for access to government information under the *Government Information (Public Access) Act 2009* (NSW) (GIPA Act).

4.4 Access to information under GIPA Act

Anyone can access government information that is held by Sydney Metro, in accordance with the GIPA Act. Sometimes the information requested can include personal and health information of the individual or of other people. There are certain considerations that are taken into account before any information is released and Sydney Metro may withhold the personal and health information of another person. For more information about the GIPA Act or making an access application, please visit Transport for NSW's website.

5 Sydney Metro's strategies for compliance and best practice

Sydney Metro adopts various strategies to implement best practice principles and comply with our obligations under the PPIP Act and the HRIP Act. These strategies recognise that privacy is a shared responsibility within the agency.

5.1 Policies and Procedures

Sydney Metro is required to set out in this Plan how Sydney Metro policies and practices are developed to ensure compliance with the requirements of privacy legislation.

This Plan sets out a number of specific elements of our privacy protection framework. Policies and practices are developed by:

- examining changes in the legislative, policy or operational environment for their impacts on Sydney Metro's privacy management
- conducting regular reviews of privacy policies and notices
- considering the privacy implications of changes to policies and systems for any procedural changes needed.

In particular, the Transport Code of Conduct outlines the responsibilities of our staff in protecting privacy in the course of their duties. All staff are provided with a copy of the Code and are regularly reminded of their obligations. The Code is available on our website and intranet.

Sydney Metro has a Data Breach Policy (see section 7) and a supporting Privacy Data Breach Response Procedure that outlines its strategy for responding to and containing eligible data breaches that compromise the security of the personal and/ or health information held.

The Sydney Metro compliance framework provides clear standards and accountabilities for a consistent and systematic approach to compliance.

5.2 Promoting privacy awareness

Sydney Metro undertakes a range of initiatives to ensure its staff, contractors and members of the public are informed of our privacy practices and obligations under the PPIP Act and the HRIP Act. Information about our privacy practices is also made available on our dedicated privacy page on Sydney Metro's website.

Sydney Metro promotes privacy awareness and compliance by:

- Publishing and promoting this Plan on our intranet and website.
- Publishing and promoting all privacy policies on our intranet.
- Maintaining a dedicated privacy page on our intranet that centralises all privacy resources for staff and provides information about what to do if staff are unsure about a privacy issue.
- Including privacy in our induction program in the modules for Code of Conduct and

Fraud and Corruption awareness.

- Providing a privacy advisory service to staff.
- Assessing privacy impacts of new projects or processes from the outset.
- Senior executives endorsing a culture of good privacy practice.
- Educating the public about their privacy rights and our obligations (for example, maintaining a dedicated privacy page on our website and providing privacy information on forms that collect personal and health information).

5.3 Review and continuous improvement

Sydney Metro consistently evaluates the effectiveness and appropriateness of its privacy practices, policies and procedures to ensure they remain effective and to identify, evaluate and mitigate risks of potential non-compliance. Senior Executives are briefed on significant privacy compliance incidents to enable communication and leadership on strategies for addressing privacy compliance risks.

Sydney Metro is committed to:

- Monitoring and reviewing its privacy processes regularly.
- Further promoting and maintaining privacy awareness and compliance.
- Encouraging feedback from our staff and customers on our privacy practices.
- Introducing initiatives that promote good privacy handling in our business practices (such as assessing privacy impacts of new projects or processes from the outset).
- Embedding good data management controls and organisational stewardship / accountability of personal and sensitive data across its lifecycle.
- Maintaining and continually expanding the scope of Transport information security management systems that align to ISO/IEC 27001:2013 standard.
- Carrying out comprehensive assessments of the risk to digital information and digital information systems that are used to process personal and health information.
- Actively promoting information security awareness to ensure all staff fully understand their responsibilities of information security compliance in their day-to-day activities.
- Making this plan publicly available as open access information under the GIPA Act.

5.4 Managing Sydney Metro's obligations and compliance risk

Sydney Metro approaches its compliance obligations across various IPPs by focusing on five main categories consisting of collection, retention & security, access & alteration, use and disclosure.

We mitigate the risk of non-compliance with the IPPs through:

- Conducting Privacy Impact Assessments to identify risks of breaching any of the IPPs/HPPs and to make recommendations to address those risks;
- Adopting a privacy-by-design approach to developing and implementing new projects and proposals to ensure best privacy practice is incorporated from the point of collection

of personal information to its use, disclosure and disposal;

- Consulting the NSW Privacy Commissioner on new projects and proposals that involve collection, use or disclosure of personal information;
- Notifying the Privacy Commissioner of data breaches that affect the personal information of Sydney Metro stakeholders;
- Reviewing privacy notices and consent forms to ensure compliance with collection obligations under the PPIP Act;
- Managing compliance risks through third parties occurs through inclusion of enforceable contractual measures in contract, Memorandums of Understanding to outline privacy compliance obligations;
- Promoting avenues for staff and community complaints in relation to a breach of privacy on the Sydney Metro website.

6 Your rights

6.1 Requesting an internal review

Any person can make a privacy complaint by applying for an 'internal review' of the conduct they believe breaches an IPP and/or a HPP. A person can also discuss any concerns with the privacy team or email sydneymetro.privacy@transport.nsw.gov.au.

Internal review is the process by which Sydney Metro manages formal, written privacy complaints about how we have dealt with personal information or health information. All written complaints about privacy are considered to be an application for internal review, even if the applicant doesn't use the words 'internal review'. If you would prefer to resolve your privacy concern informally, please let us know when you contact us (see 6.1.4 below).

6.1.1 Your rights of internal review

An application for internal review should:

- be in writing
- be addressed to Sydney Metro, and
- specify an address in Australia at which you can be notified after the completion of the review.

To apply for an internal review, you can submit the Application Form – Internal Review of Conduct in relation to a privacy breach or send your application and any relevant material by email or post to Sydney Metro.

6.1.2 Process

The internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is a staff member of Sydney Metro, and
- is qualified to deal with the subject matter of the complaint.

Internal review follows the process set out in the Information & Privacy Commission's *internal review checklist*.

When the internal review is completed, the applicant will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action we propose to take
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal (NCAT).

Sydney Metro will also:

- provide a copy of your internal review request to the Privacy Commissioner;
- send a copy of the draft internal review report to the Privacy Commissioner and take

into account any submissions made by the Privacy Commissioner;

- keep the Privacy Commissioner informed of the progress of the internal review and provide a copy of the finalised internal review report.

Further information about the internal review process is available on the IPC website *How to handle an internal review*.

6.1.3 Timeframes

You must lodge your request for internal review within six months from the time you first became aware of the conduct that you think breached your privacy. Sydney Metro may accept late applications in certain circumstances. If a late explanation is not accepted then Sydney Metro will provide you with a written explanation.

Sydney Metro will acknowledge receipt of an internal review and will aim to:

- complete the internal review within 60 calendar days, (Sydney Metro will contact you if the review is likely to take longer than 60 days to complete); and
- respond to you in writing within 14 calendar days of completing the internal review.

If the internal review is not completed within 60 days, you have a right to seek a review of the conduct by the NCAT.

6.1.4 Other ways to resolve privacy concerns

We welcome the opportunity to discuss any privacy issues you may have. You are encouraged to try to resolve privacy issues with us informally before lodging an internal review.

You can raise your concerns with us by contacting the Privacy Officer on sydneymetro.privacy@transport.nsw.gov.au.

Please keep in mind that you have six months from when you first became aware of the potential breach to seek an internal review. This six month time frame continues to apply even if attempts are being made to resolve privacy concerns informally. Please consider this time frame when deciding whether to make a formal request for internal review or continue with informal resolution.

6.2 Requesting an external review

If you are unhappy with the outcome of the internal review conducted by Sydney Metro or do not receive an outcome within 60 days, you have the right to seek an external review by the NCAT.

You have 28 calendar days from the date of the internal review decision to seek an external review under Section 53 of the *Administrative Decisions Review Act 1997* (NSW).

To request an external review, you must apply directly to the NCAT, which has the power to make binding decisions on an external review.

To apply for an external review or to obtain more information about seeking an external review, including current forms and fees, please contact the NCAT:

Website: http://www.ncat.nsw.gov.au/

Phone: 1300 006 228

(02) 9377 5711

Visit/post: Level 9, John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000

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

6.3 Complaints to the Privacy Commissioner

Individuals have the option of complaining directly to the Privacy Commissioner if you believe that we have breached your privacy.

The Privacy Commissioner's contact details are:

Office: NSW Information & Privacy Commission
Level 15, McKell Building
2-24 Rawson Place
Sydney NSW 2000

Post: GPO Box 7011

Sydney NSW 2001

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

7 Data Breaches

7.1 What is an eligible data breach?

A data breach occurs when any personal information held by Sydney Metro is lost or accessed or disclosed without authorisation.

A data breach will be an Eligible Data Breach if the breach is likely to result in serious harm to the individuals to whom the information relates.

7.2 Sydney Metro's Data Breach Policy and Privacy Data Breach Response Procedure

In the event of an actual or suspected data breach, Sydney Metro staff must comply with the Sydney Metro Data Breach Policy which prescribes the principles and requirements that must be applied by all Sydney Metro staff to meet our obligations under under the mandatory notification of data breaches scheme in Part 6A of the PPIP Act.

This requires all staff to:

- Immediately report suspected or actual privacy or data breaches to sydneymetro.privacy@transport.nsw.gov.au;
- comply with the Sydney Metro Privacy Data Breach Response Procedure, including participating in any Breach Response Team.

Members of the public or other third parties can notify Sydney Metro of a suspected data breach by emailing details to sydneymetro.privacy@transport.nsw.gov.au.

8 Key definitions

8.1 What is personal 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 recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.

Essentially, personal information is any information or an opinion that is capable of identifying an individual. Information is 'about' an individual where there is a connection between the information and the individual. Information will also be 'about' someone where it reveals or conveys something about them — even where the person may not, at first, appear to be a subject matter of the information. For example, travel or journey patterns may not be considered personal information, however, when linked to an Opal card and other public information the two could reveal the identity of the individual as well as their location, both of which are personal information.

Common examples of personal information include an individual's name, bank account details, fingerprints, or a photograph or video.

8.2 What is not personal information?

There are certain types of information that are not considered personal information and these are outlined at section 4(3) and section 4A of the PPIP Act (see also section 5 of the HRIP Act). Some of these include:

- Information about an individual who has been dead for more than 30 years.
- Information about an individual that is contained in a publicly available publication (for example, information provided in a newspaper or court judgment available on the internet).
- Information or an opinion about an individual's suitability for appointment or employment as a public sector official (for example, recruitment records, referee reports and performance appraisals).

8.3 What is health information?

Health information is a specific type of personal information that is defined in section 6 of the HRIP Act as:

- Personal information that is information or an opinion about:
    - An individual's physical or mental health or disability.
    - An individual's express wishes about the future provision of health services to themselves.
    - A health service provided, or to be provided, to an individual.
- Other personal information collected to provide, or used in providing, a health service.

- Other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances.
- Genetic information about an individual that is or could be predictive of the health (at any time) of the individual or their genetic relatives (e.g. descendants).
- Healthcare identifiers.

8.4 What is *not* health information?

As with personal information, there are certain types of information which are not considered health information. These are outlined in section 5(3) of the HRIP Act and include, for example, health information of an employee who has been deceased for more than 30 years.

8.5 Sensitive personal information

Sensitive personal information is a specific type of personal information that is defined in section 19 of the PPIP Act. It includes information about ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

8.6 Other definitions

Collection – (of personal information) the way in which Sydney Metro acquires personal or health information, which can include a written or online form, a verbal conversation, a voice recording, or a photograph.

Disclosure – (of personal information) occurs when Sydney Metro makes known to an individual or entity personal or health information not previously known by that individual or entity.

Eligible Data Breach – has the meaning given to it in section 59D(1) of the PPIP Act.

Exemptions from compliance with Information Protection Principles (IPPs) – (general, specific and other exemptions) are provided both within the principles (and under Division 2 and Division 3 of Part 2 of the PPIP Act).

Privacy principles – the Information Protection Principles (**IPPs**) set out in Division 1 of Part 2 of the PIPP Act and Health Privacy Principles (HPPs) set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Within these principles lawful exemptions are provided.

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

Note: public register exemptions are provided for in clause 7 of the *Privacy and Personal Information Protection Regulation 2014*.

Privacy obligations – the information privacy principles or the health privacy principles and any exemptions to those principles that apply to Sydney Metro, which is a public sector agency

Staff – any person working in a permanent, casual or temporary capacity in Sydney Metro, including consultants and contractors.

Use – (of personal information) occurs when Sydney Metro applies the personal information for its own purposes. This may include sharing the personal information with a contractor who uses it for Sydney Metro's purposes.

Annexure A – Accountabilities and responsibilities

Who	Responsibility
All staff	Comply with the PPIP Act and HRIP Act, including the information protection principles and health protection principles, when handling personal information. Report any suspected or actual data breach immediately to manager and sydneymetro.privacy@transport.nsw.gov.au.
All staff responsible for the management of contracts	Understand the personal information lifecycle for information dealt with under the contract. Ensure everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of any personal information by the supplier.
All staff involved in new collections or novel uses or disclosures of personal information	Contact the Privacy Team to request a privacy impact assessment and assess whether the new collection or novel use is lawful.
Breach Response Team	Provide advice and management of response to an eligible data breach in accordance with the Privacy Data Breach Response Procedure.
Business unit responsible for handling personal information and/or data custodian	*Prevention* Ensure team members are aware of personal information holdings and obligations. Develop and implement supporting tools and systems for managing personal information (may form part of business unit processes). *In event of data breach* Lead the Breach Response Team and report to senior management.

Who	Responsibility
Enterprise Security	Provide advice on cyber security controls to protect personal information. Contain breach and mitigate harm where possible. Representative on any Breach Response Team. Assist in reviewing security and monitoring controls related to any breach (for example, access, authentication, encryption, audit logs).
Division Head of area where breach originated	Receive report of possible eligible data breach. Decide if data breach is an eligible data breach.
General Counsel and Executive Director Legal – Corporate	Accountable for establishing standards, policy, guidelines, advice, training and toolkits to enable business areas to comply with this policy.
Privacy team (Legal)	Provide privacy advice and conduct privacy impact assessments as needed. Provide training, fact sheets and resources to support Sydney Metro in fulfilling its obligations under the PPIP Act and HRIP Act. Advise in the event of a data breach and establish Breach Response Team.
Information Access Unit	Conducting internal reviews as required under Part 5 of the PPIP Act.
Information Management	Provide advice on State Records requirements including retention and disposal of information. Assist in reviewing security and monitoring controls related to any breach (for example, access, authentication, encryption, audit logs) and to provide advice on recording the response to the data breach