Transport for NSW

Privacy Management Plan

November 2023

NSW GOVERNMENT

transport.nsw.gov.au

Acknowledgement of Country

Transport for NSW acknowledges the traditional custodians of the land on which we work and live.

We pay our respects to Elders past and present and celebrate the diversity of Aboriginal people and their ongoing cultures and connections to the lands and waters of NSW.

Many of the transport routes we use today – from rail lines, to roads, to water crossings – follow the traditional Songlines, trade routes and ceremonial paths in Country that our nation's First Peoples followed for tens of thousands of years.

Transport for NSW is committed to honouring Aboriginal peoples' cultural and spiritual connections to the lands, waters and seas and their rich contribution to society.

Transport Privacy Management Plan – November 2023

Objective Ref: SF2022/029116

Table of Contents

Transport Privacy Management Plan – November 2023

Objective Ref: SF2022/029116

Document control

Authors	Privacy Team, Legal, Privacy and Internal Audit
Document owner	Kate Watts, Executive Director Government Regulatory and Prosecutions
Approved by	Tracey Taylor, Deputy Secretary Corporate Services
Branch	Legal, Privacy and Internal Audit
Division	Corporate Services
Review date	November 2025
Superseded documents	Transport Privacy Management Plan – March 2022

Versions

Version	Amendment notes
1	This the first version of the Transport Privacy Management Plan on an updated template. It replaces the Transport Privacy Management Plan published March 2022 and incorporates the requirements of Part 6A of the *Privacy and Personal Information Protection Act 1998* relating to mandatory notification of data breaches.

1. Introduction

1.1 Transport's commitment to your privacy

The Transport Cluster is committed to protecting the privacy of our customers and staff through the appropriate collection and handling of personal and health information.

The Transport Cluster consists of the following agencies:

- Transport for NSW (**TfNSW**)
- Sydney Trains
- NSW Trains
- Sydney Ferries
- State Transit Authority
- Sydney Metro

This Privacy Management Plan includes TfNSW, Sydney Trains and NSW Trains (collectively referred to as Transport) and applies to the Transport Cluster except for Sydney Metro.

We protect the personal and health information we collect and hold in accordance with the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) and 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 Transport collects and how it is handled.
- Promoting staff awareness of Transport's privacy obligations through targeted campaigns, training and intranet resources.

In the event of a data breach, Transport'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 privacy related accountabilities and responsibilities of staff are contained in Appendix D.

1.2 Purpose of this Privacy Management Plan

The Plan is an important tool in explaining:

- how Transport 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 each of the agencies in Transport

Transport Privacy Management Plan – November 2023

Objective Ref: SF2022/029116

- how to access and amend your personal information; and
- what to do if a Transport agency may have breached its privacy obligations under the PPIP Act or HRIP Act.

The majority of the Plan is consistent across the agencies in Transport. Where there are differences, the differences will be set out in each section of the Plan.

In addition, this Plan acts as a reference tool for staff of Transport to explain how we can best meet our privacy obligations under the PPIP and HRIP Acts. As public sector officials, Transport 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 addresses the requirements under section 33 of the PIPP Act.

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.

Transport staff are regularly reminded of their responsibilities under the PPIP Act and HRIP Act and these obligations are reinforced in each agency's Code of Conduct and through initiatives outlined in section 5 of this Plan. This includes the delivery of regular face to face privacy training sessions to staff and promotion of Privacy Awareness Week events and an online privacy training module.

Where possible Transport enables individuals to interact with each agency anonymously, for example, when providing Transport agencies with feedback and sentiments.

1.3 About us

Transport includes TfNSW, Sydney Trains and NSW Trains (NSW TrainLink) for the purposes of this Plan.

TfNSW is responsible for strategy, integration, coordination and improving the customer experience – including planning, program administration, policy and regulation, procuring transport services, infrastructure and freight and regional development. Transport operators – including Sydney Trains and NSW Trains focus on the provision of safe, clean, reliable and efficient transport services.

Corporate Services, including privacy compliance functions for TfNSW, Sydney Trains and NSW Trains is centralised. Accordingly, one Privacy Management Plan sets out the key information handling practices for these entities. Where differences in information handling exists between agencies these have been clearly marked under the relevant Information Protection Principles.

1.3.1 TfNSW and its privacy context

TfNSW was established on 1 November 2011 under the *Transport Administration Act 1988* (NSW) (**TAA**) and is responsible for roads and maritime matters, as well as improving the customer experience, planning, program administration, policy, regulation, procuring transport services, infrastructure and freight. TfNSW also leads the procurement of transport infrastructure and oversees delivery through project delivery offices and industry delivery partners. The functions of each Transport agency are set out in the TAA.

As a NSW public sector agency, TfNSW is required by the PPIP Act to have a privacy management plan.

TfNSW sets the strategic direction for Transport agencies and works in partnership with Sydney Trains, NSW Trains, the State Transit Authority and Sydney Metro.

Guided by our Future Transport Strategy 2056, Transport leads the development of safe, integrated and efficient transport systems for the people of NSW. Our customers are at the centre of everything that we do, including transport planning, strategy, policy, procurement and other non-service delivery functions across all modes of transport.

We work hand-in-hand with our operating agencies, private operators and industry partners to deliver customer-focused services and projects and programs to reliably and safely improve the movement of people and goods by all transport modes, including through the road and freight network, NSW waterways, the public transport network, rail, ferries, light rail and point to point, and active transport such as cycling and pedestrian networks. For more information about TfNSW's functions, please visit our TfNSW website.

1.3.2 Sydney Trains and its privacy context

On 1 July 2013, Sydney Trains replaced RailCorp as the provider of metropolitan train services for Sydney. Intercity services from the Sydney CBD that were also formerly operated by RailCorp are now run by the new agency NSW Trains, who also operates regional services to destinations around NSW and Brisbane, Canberra and Melbourne. Regional services were previously operated by CountryLink.

From 1 July 2020, RailCorp was converted into the Transport Asset Holding Entity (TAHE) and established as an independent statutory State Owned Corporation. The TAHE assumes ownership of RailCorp's asset base, which is primarily comprised of heavy rail assets.

Pursuant to s 11 of the *Transport Administration (General) Regulation 2013* (**TA Regulations**), Sydney Trains has the functions of RailCorp under ss 6, 7, 9, 11 and 11A of the TAA. They include but are not limited to:

- operating railway passenger services
- holding, managing, maintaining and establishing rail infrastructure facilities
- operating other transport services, including bus services, whether or not in connection with its railway services, and

- acquiring, selling, leasing or otherwise disposing of its land.

Sydney Trains is a 'public sector agency' for the purposes of PPIPA and HRIPA, by virtue of the definitions of 'public sector agency' provided in s 3(1) of PPIPA and s4(1) of HRIPA. Sydney Trains collects, holds, uses and discloses personal and health information for the purpose of carrying out our functions.

1.3.3 NSW Trains and its privacy context

NSW Trains provides intercity and regional rail and coach services for customers travelling longer distances, who need more comfortable and reliable trains with on-board facilities. NSW Trains operates services to the Hunter, Central Coast, Blue Mountains, Southern Highlands and South Coast regions, as well as an interstate network which extends into Victoria, Queensland and the Australian Capital Territory.

Pursuant to s 33 of the TA Regulations, NSW Trains has the functions of RailCorp under ss 6, 9, 11 and 11A of the TAA. They include but are not limited to:

- operating railway passenger services
- operating other transport services, including bus services, whether or not in connection with its railway services, and
- acquiring, selling, leasing or otherwise disposing of its land.

NSW Trains is a 'public sector agency' for the purposes of the PPIP Act and HRIP Act, by virtue of the definitions of 'public sector agency' provided in s 3(1) of the PPIP Act and s 4(1) of the HRIP Act. We collect, hold, use and disclose personal and health information for the purpose of carrying out our functions.

1.4 Contact us

For further information about this Plan or any other concerns about your privacy, please contact TfNSW. You may contact us on the details below for information about:

- How Transport 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 (unless the subject of the review is the conduct of the Privacy Officer).

If TfNSW, Sydney Trains and NSW Trains staff feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Privacy team in the Legal, Privacy & Internal Audit branch.

Web: www.transport.nsw.gov.au

Post: Legal, Privacy & Internal Audit Branch
Transport for NSW

Transport Privacy Management Plan – November 2023

Objective Ref: SF2022/029116

PO Box K659
Haymarket NSW 1240

Email: privacy@transport.nsw.gov.au

2. Personal and health information held by Transport

Transport undertakes a diverse range of functions and activities. The collection of customer information is a central part of many of these functions and activities. We also have significant obligations in respect of maintaining personnel files and records of staff.

As a consequence, we hold a large amount of personal and health information about customers (including Opal card holders, licensed drivers and motorcycle riders, vehicle and vessel operators and owners of registered vehicles and vessels) and staff in a number of different locations and formats.

Transport does not maintain any public registers for the purposes of the PPIP Act or HRIP Act. Examples of the personal and health information collected and held by Transport in the exercise of each agency's functions is at **Annexure A** of this document.

The Transport Privacy team must be consulted regarding proposals to share or disclose sets of personal information held by Transport.

Transport use a number of significant information systems to handle and store personal and health information. We follow strict rules on the storage of personal and health information in order to protect it from unauthorised access, loss or other misuse. At **Annexure B** are a list of the significant information systems operated by Transport.

2.1 Personal and health information held by Sydney Trains

Sydney Trains holds a range of personal and health information in a number of locations and in a range of formats. The main kinds of personal and health information held by Sydney Trains, including a high-level explanation of how those kinds of information are related to Sydney Trains' functions and activities, are set out below:

- Sydney Trains' Customer Service Directorate holds personal and health information about customers who have been involved in incidents, such as falls, on Sydney Trains' property. This personal and health information is collected by Sydney Trains from its customers for the purposes of assisting them during and after incidents. Sydney Trains' Customer Service Directorate may also hold personal information about customers who have witnessed incidents on Sydney Trains' property and provided their accounts of the incidents to Sydney Trains.
- Sydney Trains' Customer Service Directorate holds personal information about some customers who have lost property on Sydney Trains' train carriages and other premises.
- Sydney Trains does not routinely store individualised health records about its staff who are involved in rail safety work. Health assessment reports are usually received in form of

certificates of fitness to complete rail safety work. Medical results or specialist reports are not shared with the business from the medical provider. Fitness for duty reports differ from standard health assessment certificates and are released with the written consent of the employee.

- Examples of health information held by Sydney Trains include:
    - Local business units may keep a record of occupational vaccination history for WHS purposes and to facilitate vaccination for employees as appropriate.
    - Drug and alcohol reports that require review by Chief Health Officer – Health information requested only by Chief Health Officer relating to complex medical case management. This information may be requested as per the National Standards for Assessment of Rail Safety Workers.
    - Medical certificates.
    - Fitness for duty reports requested under National Standard for Assessment of Rail Safety Workers.
- Sydney Trains Customer Service Directorate holds personal information about customers who have been issued with infringements such as fare evasion.
- Database Consultants Australia (DCA), a contractor to Sydney Trains, holds personal information about customers who have been issued with infringements such as fare evasion. DCA is contracted to Sydney Trains for the purposes of maintaining and issuing infringements, such as fare evasion, to customers by Sydney Trains' Transport Officers. The type of personal information held by DCA will include photographs of customers' identification, such as a driver's licence, that are taken by Sydney Trains' Transport Officers in the process of issuing infringements.

Sydney Trains does not maintain any public registers for the purposes of PPIPA or HRIPA.

2.2 Personal and health information held by NSW Trains

NSW Trains undertake a diverse range of functions and activities. The collection of customer information is a central part of many of these functions and activities. NSW Trains also have substantial obligations in respect of maintaining personal files and records of our staff. As a consequence, NSW Trains holds a range of personal and health information about customers and staff in a number of locations and in a range of formats.

The main types of personal and health information held by NSW Trains include:

- Personal and health information about customers related to booking details, including name, phone, address, email, pension numbers, concession card numbers, entitlements, disabilities, medical requirements for on-board, mobility requirements, and bookings with other suppliers (e.g. hotel, rail authorities).
- Personal and health information related to Anti-Discrimination Board complaints, appeals to the NSW Civil and Administrative Tribunal, contractors and consultants engaged by business units, disciplinary records, grievance records, informal information for the management of poor work performance or conduct, workers compensation and

rehabilitation records; and personal and health information related to insurance or legal claims by members of the public.

Note: personal and health information related to medical records, performance development, leave applications, Equal Employment Opportunity, etc. are held by Transport Shared Services. NSW Trains do not maintain any public registers for the purposes of PPIPA or HRIPA.

3. How Transport manages personal and health information

This section describes how Transport uses, discloses and stores personal and health information in alignment with its functions and activities, and with standards which Transport 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 section 8 .

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 and health information unless we need it. We will especially avoid collecting sensitive personal information if we don't need it. By limiting our collection of personal and health information to only what we need, it is much easier to comply with our other obligations.

- Example: when designing a form, ask yourself: "do we really need each piece of this information?"
- Example: If we need to know an individual's age only to provide age-appropriate services, we will ask for their age, age decile or year of birth, not their exact date of birth.

Since we only ask for personal and health information when we need it to perform our functions, we may not give individuals the opportunity not to identify themselves. For example, we need to know when employees have a health condition; and we need to confirm students are entitled to free travel or a concession.

Where it is possible for us to transact with you anonymously (e.g customer feedback, journey planning, etc) we will ensure this opportunity is provided to you.

We will ensure that the personal and health information we collect is relevant, accurate, up-to-date, complete, and not misleading, excessive and unreasonably intrusive. We will do this by providing privacy training to all staff and will conduct audits of the collection, use and disclosure of personal and health information.

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 instead collect personal information from the individual's parent or guardian; or
- It would be unreasonable or impracticable to collect information directly from the individual.

We will only collect information for lawful purposes relating to our functions and activities. The functions and activities of each of the Transport agencies are set out in legislation governing our operations. A list of the legislation applicable to Transport can be accessed through this link: Legislation | Transport for NSW.

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. Training our staff is one important way we do this.

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. We rely on the person providing the information to confirm its accuracy and sometimes we will independently verify the information depending on the reliability of the source of the information, the lapse in time between the point of collection and any proposed use or disclosure of the information.

For example, individuals applying for an Opal card are provided with detailed information on why information is collected and how it will be used and disclosed. For specific information on how TfNSW manages the information collected under the Opal Electronic Ticketing System, please refer to the Opal Privacy Policy.

Data is also collected from third parties, such as other NSW government agencies providing contracted services to clients on behalf of Transport and agencies in other jurisdictions. The data may include personal and health information collected, used and disclosed for policy making, program and service planning, service delivery, monitoring and reporting, program and service evaluation and research.

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.***

When we use personal and health information, it means that we use it internally within the agency forming part of Transport. This includes the provision of information to contractors engaged by TfNSW to manage information on our behalf in circumstances where TfNSW retains control over the handling and use of the information.

We will only use personal and health information for:

- The primary purpose for which it was collected
- A directly related purpose
- Another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health of the individual to whom the information relates or of another 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 Transport 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 of the agency forming part of Transport. We will only disclose personal information if:

- The disclosure is directly related to the purpose for which the information was collected; or

- The individual has been made aware in the 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.

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" principle for privacy purposes. Where Transport agencies provides information to another person or body, including another agency within the Transport cluster, this will constitute a "disclosure" principle for privacy purposes.

Transport 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 Transport privacy officer.

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 deidentify all personal information before seeking advice from another agency or will obtain prior consent from the individual who the information is about before disclosure or may 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.

For example, we have a memorandum of understanding with NSW Police Force which sets out the basis on which TfNSW will disclose information from the Opal electronic ticketing system. It sets out when and how NSW Police Force will request information and how we will respond. Both agencies must continue to comply with the PPIP Act and HRIP Act and must also keep records so that each can audit requests and responses for personal information. We report on the most recent audit in our annual report.

The HPPs also contain information regarding 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. Generally, disclosure is made to a party in another jurisdiction where there is a mutual recognition scheme and transfers of information are subject to agreements, consent or where there is a comparable privacy framework.

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 otherwise when:

- The individual has consented to the disclosure;
- 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; 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 information we anonymise it first. For example, with approval from Data Custodians / Data Owners and relevant Ethics Committees, the Centre for Road Safety utilises identifiers to link crash data. The use of such identifiers is essential to our function of conducting research in connection with and implementing programs, projects and strategies for promoting and improving road safety.

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.***

Transport stores information in a variety of ways, including on each of the Transport agencies' databases, cloud storage by third parties and in various physical locations.

Some of the security measures taken by Transport 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.
- Print on demand (secured 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, NSW Data Sharing Act* 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.

Transport Privacy Management Plan – November 2023

Objective Ref: SF2022/029116

- When no longer required, we destroy information in a secure manner as appropriate (for example, using secure (locked) recycling bins and shredders).
- 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 would prevent them from unauthorised use or disclosure of information that we hold.
- Providing mandatory information security awareness training to Transport staff.
- Monitoring of usage through access logs and regular audits.
- Training for data protection and use.
- Monitoring of data feeds and transfers.
- Logging of where personal information is through data management tooling.

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

3.4 Additional Health Privacy Principles

HRIP Act HPPs 12, 13 & 15
An agency must:

- ***Only assign health identifiers to individuals if reasonably necessary to enable it to carry out its functions efficiently***
- ***Give an individual the opportunity not to identify themselves with respect to health services or transactions***
- ***Not include a health record in a health record linkage system without consent, nor disclose an identifier without consent***

Identifiers are used to uniquely identify an individual and their health records. An identifier does not need to use a person's name as they are designed to be unique to a specific individual (for example, a customer number, unique patient number, tax file number, or driver licence number).

For example, with approval from Data Custodians / Data Owners and relevant Ethics Committees, the Centre for Road Safety utilises identifiers to link crash data obtained from NSW Police with hospitals admissions data obtained from NSW Health to identify serious injuries resulting from road crashes on NSW. The use of such identifiers is essential to our function of conducting research in connection with and implementing programs, projects and strategies for promoting and improving road safety.

We will only use health records linkage systems when individuals have expressly consented to their information being included on such a system, or for research purposes which have been approved by an Ethics Committee and in accordance with the NSW Privacy Commissioner's Statutory Guidelines on Research.

For example, the Centre for Road Safety undertakes ongoing linkage of health datasets to road crash data for the purposes of developing practical solutions which reduce death and injuries on NSW roads. Such linkage was reviewed and approved by the NSW Population and Health Services Research Ethics Committee and a waiver of individual consent was granted.

Notification is usually provided to individuals through a 'privacy notice' at the initial time of collection or as soon as we can afterwards. Privacy notices can be in writing or verbal. Generally, privacy notices are included on an application form used to collect information, or in the case of inbound calls to call centres, a recorded message or verbal notice.

If we collect personal or health information from a non-English speaking background individual, the Community Language Privacy Notice should be used. The Information & Privacy Commission's Best Practice Guide Privacy and People with Decision-making Disabilities explains how to notify a person who has limited capacity to understand.

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

3.5.1 Exemptions from IPPs

PPIP Act sections 22-28 relating to law enforcement and related matters; ASIO; investigative agencies; lawful authorisation; where non-compliance benefits and 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 Transport 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.

Transport is also permitted by law to disclose personal information in accordance with certain exemptions. Examples of the exemptions which allow for Transport to disclose personal information are at **Annexure C**.

3.5.2 Exemptions from HPPs

Exemptions are located mainly in Schedule 1 of the HRIP Act and may allow Transport 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.

3.5.3 Codes of practice or public interest directions

There are no privacy codes of practice or public interest directions that apply to Transport.

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 Transport holds about them. They also have the right to change their own personal and/or health information Transport holds, for example, updating their contact details. However, if a Transport agency 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.

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

There is no fee to access or amend your personal and/or health information.

This section explains how to request access to your own information via an informal or formal application.

Transport encourages you to keep your personal and/or health information up-to-date and accurate, particularly information about your personal contact details and next of kin contact details so that you (or they) can be contacted in an emergency. It is also your responsibility to inform us if you wish to change your bank account details or payment details.

4.1 Members of the public

Often we rely on the person providing the information to confirm its accuracy. Sometimes we will independently verify the information (for example a concession entitlement). 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, or accessing an online account or website, such as the Opal website. If you do not know which business unit within Transport to contact about your request or your request has been denied, please fill out and submit an Application Form – Access or email 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 does 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 Transport to disclose their personal information to someone else who would not normally have access to it.

Under section 7 and section 8 of the HRIP Act, an 'authorised representative' can act on behalf of someone else.

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 Transport in accordance with the GIPA Act. Sometimes the information requested can include personal and health information of other people. There are certain considerations that are taken into account before any information is released and Transport may withhold the personal and health information of another person. For more information about the GIPA Act or making an access application, please visit our website.

5. Strategies for compliance and best practice

Transport adopts several 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.

Transport Privacy Management Plan – November 2023

Objective Ref: SF2022/029116

5.1 Policies and Procedures

Transport is required to set out in this plan how policies and practices are developed to ensure compliance by the agency 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 Transport'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, Transport's 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.

The Opal Privacy Policy outlines the responsibilities of our staff in protecting the privacy of our Opal customers. All staff and contractors working on the Opal travel system are regularly reminded of their obligations. The Opal Privacy Policy is available on our website.

Transport has a Data Breach Policy (see section 7) and a supporting Privacy Data Breach Response Procedure that outlines Transport agencies' strategy for responding to and containing Eligible Data Breaches that compromise the security of the personal and/ or health information held.

This Plan has been developed in alignment with the proposed TfNSW Enterprise Data Governance and Management Framework. The TfNSW Enterprise Data Governance and Management Framework will outline the people, processes, data and technology requirements for effective enterprise-wide data management and allocates roles and responsibilities to identified data owners / stewards for high value systems and data. The TfNSW Enterprise Data Governance and Management Framework also defines the roles and accountabilities around the handling of personal information. Annexure B outlines the major information holdings.

This plan is consistent with TfNSW's Enterprise Compliance Framework. The Enterprise Compliance Framework provides clear standards and accountabilities for a consistent and systematic approach to compliance.

5.2 Promoting privacy awareness

Transport agencies undertake 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 each of Transport agencies' websites.

Transport agencies promote privacy awareness and compliance by:

- Publishing and promoting this plan on our intranet and website.

- Including privacy in our induction program in the modules for Code of Conduct and Fraud and Corruption awareness.
- 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.
- Drafting and publishing privacy factsheets on our intranet to provide staff with practical guidance on privacy issues and considerations.
- Delivering periodic face to face training across different business areas. Training attendance is captured in the employees personal learning record or by privacy team.
- Providing a dedicated privacy advisory service to staff.
- Assessing privacy impacts of new projects or processes from the outset. The privacy impact assessment process is linked in with procurement, cyber security and project authorisation to ensure a privacy by design approach is embedded.
- Senior executives endorsing a culture of good privacy practice. Senior Executives are involved in Privacy Awareness Week events in promoting a culture of privacy compliance.
- 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

Each Transport agency 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.

Transport agencies are 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 promote 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 TfNSW's obligations and compliance risk

Transport's compliance obligations across various IPPs can be broken into five main categories consisting of collection, retention & security, access & alteration, use and disclosure .

Mitigating risk of non-compliance with the various IPPs is promoted through the use of the following mechanism:

- The conduct of Privacy Impact Assessments on a regular basis to identify any actual or potential risk to a breach of the IPPs/ HPPs and the implementation of recommendations to address the risk;
- Adopting a privacy-by-design approach to the development and implementation of all 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;
- Mandatory Privacy Training is promoted across the agency in addition to bespoke privacy training delivered to staff with exposure to sensitive personal information or a large volume of personal information. A training record is retained against a specified Privacy Course ID;
- The NSW Privacy Commissioner is consulted on new projects and proposals that involve the collection, use or disclosure of personal information;
- Transport notifies the privacy commissioner of data breaches that impact the personal information of Transport stakeholders;
- Privacy notices and consent forms are reviewed to ensure compliance with the collection obligations in 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 and where appropriate annual proactive auditing and reporting requirements;
- Compliance with the State Records Act and the NSW Government Cloud Strategy l are ensured through Cyber Security Assessments and engagement with NSW State Archives in conjunction with the conduct of Privacy Impact Assessments to ensure consistent and best practice compliance.
- Avenues for staff and community complaints in relation to a breach of privacy are promoted on the Transport agency website
- The Agency conducts proactive compliance audits in relation to the handling of customer personal information
- The agency is developing a privacy strategic plan to assess and uplift privacy compliance and maturity across Transport;

- A clear reporting pathway for privacy is in development to provide visibility at the senior executive level of compliance standards across the agency.

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 privacy@transport.nsw.gov.au.

Internal review is the process by which a Transport agency 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 TfNSW, Sydney Trains or NSW Trains
- 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 TfNSW.

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 TfNSW, Sydney Trains or NSW Trains (as applicable), 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).

A Transport agency is also required to:

- 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 will 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. A Transport agency may accept late applications in certain circumstance. If a late explanation is not accepted then the Transport agency will provide you with a written explanation.

Transport agency will acknowledge receipt of an internal review and will aim to:

- Complete the internal review within 60 calendar days, (Transport agency 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 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 TfNSW 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

Haymarket 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 Transport 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 Transport's Data Breach Policy and Privacy Data Breach Response Procedure

In the event of an actual or suspected data breach, Transport staff must comply with the Transport Data Breach Policy which prescribes the principles and requirements that must be applied by all Transport staff to meet our obligations 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 privacy@transport.nsw.gov.au;
- comply with the Transport Privacy Data Breach Response Procedure, including participating in any Breach Response Team.

Members of the public or other third parties can notify Transport of a suspected data breach by emailing details to 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 a Transport agency 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 a Transport agency makes known to an individual or entity personal or health information not previously known by that individual or entity who use the personal or health information for their own purposes.

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).

Eligible Data Breach has the meaning given to it in section 59D(1) 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 Transport, which is comprised of three public sector agencies.

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

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

Annexure A – Personal and health information held by TfNSW

Examples of personal information collected and held by TfNSW in the exercise of its functions are as follows:

Transport for NSW on behalf of the Transport	
Staff and recruitment During the recruitment process and throughout employment, information (including personal and/or health information) is collected from applicants and staff members for various reasons such as leave management, workplace health and safety and to help TfNSW operate with transparency and integrity. Successful applicants are invited to fill out various forms in order to commence employment at TfNSW. The forms 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 • Garnishee orders • Salary sacrifice paperwork • Superannuation details • Leave details (medical certificates) • Payslips • Higher duties applications • Emergency contact details (including telephone number, postal and email address) • Leave requests • Discipline and conduct information • Performance Management and Evaluation 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 • Performance and development information • Family and care arrangements • Secondary employment • Conflicts of interest • Financial information for payroll purposes • Employment history • Criminal background checks • Passport, drivers' licence • Medicare card • Covid Declaration 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. TfNSW still treats this information confidentially.
Rail Industry Worker information TfNSW is a Registered Training Organisation and delivers rail safety training. It also collects and holds personal information about the qualifications and identity of rail safety workers in order to monitor and manage their participation in rail safety work, including access to the rail corridor.	• Personal Information collected via the Rail Industry Worker cardholder scheme • Name • Contact information

	• Qualifications • Visa status • Health information
Injury and Claims Management TfNSW collects and holds personal information for the purpose of managing workers compensation claims by Transport staff, for rehabilitation and for managing injured workers' return to work. TfNSW provides claims management and return to work services to the entire Transport through its shared services team. TfNSW deals with claims information as an agent of the relevant workers compensation insurer for each agency. Otherwise, TfNSW holds appropriate delegations from each agency to act on its behalf.	• 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 TfNSW collects information, including personal information, when receiving complaints, investigating and making decisions about staff conduct matters.	• 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 • Health records • Investigation reports which may include the above information

Transport for NSW	
Community and stakeholder engagement / communications TfNSW collects information, including personal information, when consulting with stakeholders at industry and community forums and when receiving and responding to correspondence.	• 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) • Survey responses and customer sentiment information, complaints and feedback.
Road Safety TfNSW collects information, including personal and health information, indirectly from Police and from NSW Health for the purpose of carrying out its various road safety functions, including undertaking research into road safety and developing road safety policy.	• Alcohol and drug test results for drivers obtained from NSW Health for the purposes of monitoring illegal alcohol and drug involvement in crashes • Personal information on people involved in road crashes obtained from NSW Police Force

	• Health information for NSW road crash casualties under ethics research approval (for purposes such as identifying and studying road crash injuries to improve road safety) • Personal information about road safety ambassadors whose family or friends have been involved in fatal road crashes • Information about community organisations who apply to, and participate in, the Community Road Safety Grants program
Various TfNSW occasionally holds community events or participates in events held by other agencies or organisations. During these events, TfNSW may collect information on a voluntary basis about 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, Representatives and key personnel under contracts • Contact details of people who have written to or emailed the Minister, with details of the nature of their correspondence. • Copies of replies to correspondence and records of who, if anyone, their correspondence was referred to • 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 TfNSW owns and maintains the websites: • www.transport.nsw.gov.au • www.rms.nsw.gov.au • transportnsw.info • testyourtiredself.com.au • ridetolive.com.au • roadsafety.transport.nsw.gov.au	• Website data • Photos or filming of events (TfNSW will seek permission from people before taking photos or filming events and advise them how TfNSW will manage the images and what they will be used for. Those who agree can be asked to sign a consent form).

• whatsyourplanb.net.au • maritimemanagement.transport.nsw.gov.au • towardszero.nsw.gov.au • mysydneycbd.nsw.gov.au • drivewithstatetransit.com.au • childcarseats.com.au • motocap.com.au • pacifichighway.nsw.gov.au This website is used to publish resources to help our stakeholders understand what we do. TfNSW does not publish personal or health information on the website without permission.	
Information and Ticketing TfNSW collects information, including personal information, to operate the Opal electronic ticketing system in the Greater Sydney Area. The Opal ticketing system uses a contactless smartcard or an approved payment device to provide customers with a secure, effective and efficient public transport electronic ticketing system which complies with TfNSW's obligations under the privacy legislation. TfNSW collects personal information including contact and payment card information for registered Opal card holders. Opal travel history may include personal information in some circumstances.	• Date of birth (required to assess concession eligibility on public transport) • Travel and Transport Usage • Health Information (to assess eligibility for transport concession and subsidy schemes, such as Taxi Transport Subside Scheme and School Student Transport Scheme) • Relationship and custody details in relation to school children to assess eligibility under the School Student Transport Scheme • Opal customer personal information, including but not limited to • Customer's name • Customer's Address • Travel (location) history • Customer's entitlement status • Customer travel payment data • Customer's mobile number

	• Customer's email address • Customer's credit card details • Centrelink number
Tolling TfNSW operates the E-Toll system, conducting over 140 million transactions each year and delivers tolling services for over 42 million toll trips over the Sydney Harbour Bridge each year.	• Account holder information for e-tag and tagless toll accounts • Vehicle and trip data collected from tolling cameras and e-Tag readers
Compliance and Regulatory Operations for roads and for maritime TfNSW collects a range of information, including personal information, for its regulatory functions including driver licensing, vehicle and vessel registration, automated road camera enforcement programs and administration of the Authorised Inspection Scheme for inspection of registrable vehicles.	• Driver licence status and history, including interstate or international licenses, suspensions, cancellations, disqualifications and demerit points • Driver Authorities and associated records for bus drivers and driving instructors • Vehicle registration information, including register for written off vehicles • Licensing photographs under Part 3.5 of the Road Transport Act 2013 • Information about driving offences and any resulting periods of incarceration • Information about criminal history of occupational licence holders (such as tow truck, public passenger service operators and drivers, driving instructors or authorised vehicle inspectors) • Information on licensing and registration of vessels, including aquatic and mooring licences, boat driver/marine pilot licences • Information collected from enforcement cameras • Information collected from infrastructure security cameras • Health information (such as eyesight test results and medical reports for license applications, renewals and permits)

	• Records details of Authorised Examiners under Authorised Inspection Station Scheme
Customer Surveys and Sentiments TfNSW collects personal information by conducting surveys of the travel habits of the members of households which agree to participate in the survey.	• Personal information for respondents of the annual Household Travel Survey • Customer satisfaction surveys • Customer research initiatives and sentiments obtained through social media
Learning and Development TfNSW collects information, including personal information, in order to deliver training and maintain its status as a Registered Training Organisation under the Commonwealth training regime.	• 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

Annexure B – Significant Information Systems

Significant information systems operated by TfNSW include:

Significant Information System	Description of System
SAP Corporate	HR and Finance Systems
VJ-FleetWave	Fleet Management System and FBT Calculator
Objective and/or DeskSite	Document Management System
Correspondence Management System	Automated system to register and action incoming Departmental correspondence
Image Library	Online Image Library to store and catalogue photos, images, videos, sound and logos
Rail Industry Worker System (ARA and MTA)	System to administer and manage the national safety and competency management program for Australian rail industry workers
Job Ready Plus	Student management system for managing TfNSW student and training records
DRIVES	Central system for motor vehicle registration and driver licensing in NSW.
Camera Enforcement System (CES)	Records enforcement camera images and data. Includes CCTV live images.
Electronic Toll Collection System (ETCS)	System to manage the administration of TfNSW e-tags and tag-less tolling accounts
Toll Compliance Management (TCM)	Toll infringement system
Transport Information System (TIMS)	System to record details of bus driver authorities and driving instructors, including medical records and complaints against bus drivers
OneGov (formally Government Licencing System)	Maritime licensing and registration database for all boat licensing and registrations, including mooring licences
Microsoft Teams	Microsoft Teams is the chat-based workspace in Office 365 that integrates all people, content, and tools. Teams is used TfNSW wide.
Opal Electronic Ticketing System (Opal)	The system used for ticketing for Opal cards and which is governed by the Opal Privacy Policy.
Eagle Investigation Case Management System (Eagle)	The investigation and case management system used by the Maritime Investigations Unit (MIU).

Annexure C – Exemptions to limits on disclosure of personal information

TfNSW is permitted by law to make the following disclosures of personal information:

Traffic Offences	When a non-NSW driver commits an offence in NSW we can disclose that to the driver's home jurisdiction[1]
Service NSW	We can disclose information to Service NSW so it can exercise customer service functions for us[2]
National Exchange of Vehicle and Driver Information System (NEVDIS)	We can disclose personal information (other than photos) from our Driver Licence, Demerit Point, Registrable Vehicles and Photo Card Registers to the NEVDIS[3]
Taxis Hire Cars & Buses	We can disclose licence and compliance information if reasonably necessary for the purposes of the *Passenger Transport Act 2014*[4] or the safe operation of a bus service.[5] We can also share certain information with WorkCover, NSW Police Force and safety regulators, for example breaches of the *Passenger Transport Act 2014*[6]
Document Verification Service (DVS)	We can collect/disclose information to/from DVS members to verify POI documents[7]
Driver Licence Check	We can enter agreements approved by the Privacy Commissioner disclosing licence and demerit point information to approved third parties (e.g. the driver's employer)[8]
CTP Demerit Points Disclosure Agreements	We can disclose demerit point information to CTP insurers under a Demerit Point Disclosure Agreement[9]
CTP Insurance	We can release vehicle registration information and operator's date of birth to CTP insurers in connection with the issue of policies and quotes[10]

[1] ss29(3)-(4) *Road Transport Act 2013* (however the reverse does not apply so if a NSW driver commits a traffic offence in another State the other State must either obtain the driver's details from NEVDIS or apply to TfNSW relying on the PPIP Act law enforcement exception)
[2] ss.14(4) and (8) *Service NSW (One-stop Access to Government Services) Act 2013*
[3] *Road Transport (Driver Licensing) Regulation 2017* cl. 102 & *Road Transport (Vehicle Registration) Regulation 2007* cl. 135 and *Photo Card Regulation 2014* cl. 12
[4] s.171 *Passenger Transport Act 2014*
[5] s.52D *Transport Administration Act 1988*
[6] s.171 *Passenger Transport Act 2014*
[7] *Road Transport (Driver Licensing) Regulation 2017* cls. 114 and 115
[8] *Road Transport (Drivers Licensing)Regulation 2017* clause 112
[9] *Road Transport (Driver Licensing) Regulation 2017* clause 113
[10] *Road Transport (Vehicle Registration) Regulation 2017* clause 136, and ss. 14 and 19 *Motor Accidents Compensation Act 1999*

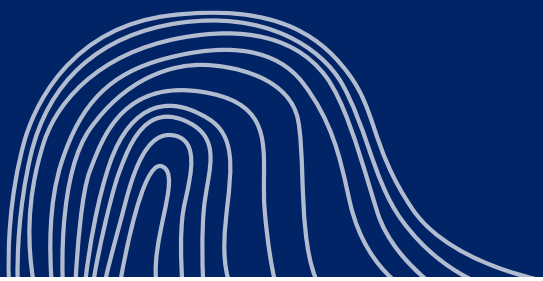
Electoral Roll	We can release data from the Driver Register to the AEC[11]
Jury Roll	We can release customer information to the Sheriff's Office to assist prepare the Jury Roll[12]
Toll Defaulters	We can disclose registration information to toll operators in the case of serious toll defaulters[13]
SNP Concessionaire	We can disclose information in connection with the operation of the concession[14]
Concession Verification	We can verify concession claims with Centrelink[15]
Rego Check	We can disclose registration information in the online services known as Free Rego Check and NSW Rego App[16]
NSW Housing	We can release information to NSW Housing for fraud investigation[17]
Heavy Vehicles	We can disclose licence, registration and compliance information for the purposes of the *Heavy Vehicle National Law* (as a delegate of the National Heavy Vehicle Regulator)[18]
NSW Police	We can disclose information for law enforcement purposes[19].
Investigate Crime	We can collect and disclose personal information for the purposes of the *Workplace Surveillance Devices Act 2007* (NSW) which allows for the use of surveillance devices to investigate crime and to enable evidence to be obtained of the commission of such crime or the identity or location of the offender(s).
State Archives and Records Authority	We can disclose records to the State Archives and Records Authority, where the Authority is entitled to control (e.g. because the record is no longer in use for official purposes), we are required to make the record available to the Authority. It must comply with any guidelines issued by the Authority in relation to how State records are to be made available as per section 29 *State Records Act 1998* (NSW).

[11] *Road Transport (Driver Licensing) Regulation 2017* clause 103
[12] ss. 75A(2B)-(2D) *Jury Act 1977*
[13] *Road Transport (Vehicle Registration) Regulation 2017* clause 133
[14] *Road Transport (Vehicle Registration) Regulation 2017* clause 33
[15] *Road Transport (Vehicle Registration) Regulation 2017* clause 137
[16] *Road Transport (Vehicle Registration) Regulation 2017* clause 138
[17] s. 69B *Housing Act 2001*
[18] *Heavy Vehicle National Law (NSW)*
[19] *Road Transport Act 2013.*

Annexure D – Privacy related accountabilities and responsibilities

Who	Responsibility
All staff	Comply with the PPIP Act and HRIP Act, including the information protection principles, when handling personal information. Report any suspected or actual data breach immediately to manager and 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 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.
Cyber Security	Provide advice on cyber security controls to protect personal information Contain breach and mitigate harm where possible Representative on any Breach Response Team
Deputy Secretary, Corporate Services	Accountable for setting the strategic direction for the Transport agencies meeting their compliance obligations.
Division Head of area where breach originated	Receive report of possible Eligible Data Breach Decide if data breach is an Eligible Data Breach
Chief Legal Officer and Executive Director Legal, Government Regulatory and Prosecutions	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 the Transport agencies in fulfilling their obligations under the PPIP Act and HRIP Act. Advise in the event of a data breach and establish Breach Response Team

Who	Responsibility
Information Access Unit	Conducting internal reviews as required under Part 5 of the PPIP Act.
Information and records 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



NSW GOVERNMENT