



Privacy Management Plan

Transport for NSW

March 2020

Contents

1	Introduction.....	4
1.1	Purpose.....	4
1.2	About us.....	4
1.3	Contact us.....	5
2	Personal and health information held by TfNSW.....	6
3	How TfNSW manages personal and health information.....	7
3.1	Collection of personal and health information – key principles.....	7
3.2	Use and disclosure of personal and health information – key principles	8
3.3	Retention and Security.....	10
3.4	Additional Health Privacy Principals.....	11
3.5	Exemptions from the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs).....	12
3.5.1	Exemptions from IPPs.....	12
3.5.2	Exemptions from HPPs.....	12
3.5.3	Codes of practice or public interest directions.....	12
4	How to access and revise your information.....	13
4.1	Members of the public.....	13
4.2	Employees.....	13
4.3	Accessing or amending other people’s information.....	14
4.4	Access to information under GIPA Act.....	14
5	TfNSW’s strategies for compliance and best practice.....	15
5.1	Policies and Procedures.....	15
5.2	Promoting privacy awareness.....	15
5.3	Review and continuous improvement.....	16
6	Your rights.....	17
6.1	Requesting an internal review.....	17
6.1.1	Your rights of internal review.....	17
6.1.2	Process.....	17
6.1.3	Timeframes.....	18
6.1.4	Other ways to resolve privacy concerns.....	18
6.2	Requesting an external review.....	18
6.3	Complaints to the Privacy Commissioner.....	19
7	Key definitions.....	20
7.1	What is personal information?.....	20
7.2	What is not personal information?.....	20
7.3	What is health information?.....	20
7.4	What is not health information?.....	21
7.5	Sensitive personal information.....	21
7.6	Other definitions.....	21

Annexure A – Personal and health information held by TfNSW	22
Annexure B – Significant Information Systems	30
Annexure C – Exemptions to limits on disclosure of personal information	32

Author:	Privacy Team, Legal, Privacy & Information Access Branch
Date:	March 2020
Division:	Corporate Services
Review	March 2022

1 Introduction

1.1 Purpose

Transport for NSW (**TfNSW**) takes the privacy of our staff and the people of NSW seriously. This Privacy Management Plan is an important tool in explaining how TfNSW upholds and respects the privacy of our customers, staff and others about whom we hold personal information. The Plan also explains who you should contact with questions about the information collected and held by TfNSW, how to access and amend your personal information and what to do if TfNSW may have breached its privacy obligations under the *Privacy and Personal Information Protection Act 1998* (NSW) (**PIIP Act**) or the *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**).

In addition, this Plan acts as a reference tool for staff of TfNSW to explain how we can best meet our privacy obligations under the PPIP and HRIP Acts. As public sector officials, TfNSW staff are required to comply with the PPIP and HRIP Acts. This Plan is intended to assist staff to understand and comply with their obligations under those Acts.

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.

TfNSW'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.

1.2 About us

TfNSW was established on 1 November 2011 under the *Transport Administration Act 1988* (NSW) (**TAA**) and is responsible for 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 cluster agency are set out in the TAA.

On 1 December 2019, Roads and Maritime Services (**RMS**) was dissolved and its assets, rights, liabilities and functions were transferred to TfNSW.

As a NSW public sector agency, TfNSW is required by the PPIP Act to have a privacy management plan. Each Transport operating agency has its own plan which is available on the respective agency's website.

TfNSW sets the strategic direction for the Transport cluster and works in partnership with Sydney Trains, NSW Trains, State Transit Authority, Sydney Metro, Point to Point Commission and Office of Transport Safety Investigations. All of these agencies, together with TfNSW, comprise the Transport cluster.

We lead 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](#) and (until January 2021) our [Roads and Maritime website](#).

1.3 Contact us

For further information about this Plan or any other concerns about your privacy, please contact TfNSW. You may contact the Privacy Officer for information about:

- How TfNSW 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).

on the details below.

If TfNSW 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 & Information Access branch.

Web: www.transport.nsw.gov.au

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

Email: privacy@transport.nsw.gov.au

2 Personal and health information held by TfNSW

TfNSW 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 substantial 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.

TfNSW 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 TfNSW in the exercise of its functions is at **Annexure A** of this document.

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

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

3 How TfNSW manages personal and health information

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

We will ensure that the personal and health information we collect is relevant, accurate, up-to-date, complete, and not misleading.

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 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.

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](#).

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* TfNSW. 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.

When we disclose information, it means that we give it to a third party *outside* TfNSW to use the information for their own purposes. 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.

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.

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 should 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 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.*

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

Some of the security measures taken by TfNSW 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* 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.
- 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 TfNSW staff.

3.4 Additional Health Privacy Principals

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 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 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.

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 TfNSW 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.

TfNSW is also permitted by law to disclose personal information in accordance with certain exemptions. Examples of the exemptions which allow for TfNSW 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 TfNSW 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 TfNSW.

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

TfNSW 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.

TfNSW 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 TfNSW 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 fnswhr@transport.nsw.gov.au

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 TfNSW to disclose their personal information to someone else who would not normally have access to it.

Likewise, under section 7 and section 8 of the HRIP Act, an 'authorised representative' can act on behalf of someone else. The HPPs also contain information regarding other reasons TfNSW 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 TfNSW 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 TfNSW 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 TfNSW's strategies for compliance and best practice

TfNSW 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.

5.1 Policies and Procedures

TfNSW 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 TfNSW'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, TfNSW'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.

5.2 Promoting privacy awareness

TfNSW 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 are also made available on our dedicated privacy page on TfNSW's [website](#).

TfNSW promotes 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.

- Providing a dedicated 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

TfNSW 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.

TfNSW 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).
- 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.

TfNSW holds a Transport wide Privacy Forum comprising of representatives from all Transport agencies. The Forum meets to discuss privacy issues and identify opportunities for better practice in protecting privacy.

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 TfNSW 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
- 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, 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).

TfNSW is also required to:

- provide a copy of your internal review request to the Privacy Commissioner.

- TfNSW will also send a copy of the draft internal review report to the Privacy Commissioner and take into account any submissions made by the Privacy Commissioner.
- TfNSW will 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. TfNSW may accept late applications in certain circumstance. If a late explanation is not accepted then TfNSW will provide you with a written explanation.

TfNSW will acknowledge receipt of an internal review and will aim to:

- Complete the internal review within 60 calendar days, (TfNSW 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 17, 201 Elizabeth Street

Sydney NSW 2000

Post: GPO Box 7011

Sydney NSW 2001

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

7 Key definitions

7.1 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.

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

7.2 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).

7.3 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 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.

7.4 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.

Personnel files containing fitness for work certificates are not considered to be health information.

7.5 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.

7.6 Other definitions

Collection – (of personal information) the way in which TfNSW 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 TfNSW 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).

Privacy principles – the Information Protection Principles (IPPs) set out in Division 1 of Part 2 of the PPIP 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 TfNSW, which is a public sector agency

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

Use – (of personal information) occurs when TfNSW applies the personal information for its own purposes. This may include sharing the personal information with a contractor who uses it for TfNSW'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 Cluster	
<p>Staff and recruitment</p> <p>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.</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> • 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

	<ul style="list-style-type: none"> • 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 <p>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.</p>
<p>Rail Industry Worker information</p> <p>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.</p>	<ul style="list-style-type: none"> • Personal Information collected via the Rail Industry Worker cardholder scheme • Name • Contact information • Qualifications

	<ul style="list-style-type: none"> • Visa status • Health information
<p>Injury and Claims Management</p> <p>TfNSW collects and holds personal information for the purpose of managing workers compensation claims by Transport cluster staff, for rehabilitation and for managing injured workers' return to work. TfNSW provides claims management and return to work services to the entire Transport cluster through its shared services team.</p> <p>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.</p>	<ul style="list-style-type: none"> • 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
<p>Workplace Conduct and Investigations</p> <p>TfNSW collects information, including personal information, when receiving complaints, investigating and making decisions about staff conduct matters.</p>	<ul style="list-style-type: none"> • 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)

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)

	<ul style="list-style-type: none"> • 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 • Information collected from Safe-T-Cams and Average Speed Cameras of the movement of all heavy vehicles
<p>Various</p> <p>TfNSW occasionally holds community events or participates in events held by other agencies or organisations.</p> <p>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.</p>	<ul style="list-style-type: none"> • 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
<p>Website publishing, photography and media</p> <p>TfNSW owns and maintains the websites: www.transport.nsw.gov.au www.rms.nsw.gov.au transportnsw.info testyourtiredself.com.au ridetolive.com.au</p>	<ul style="list-style-type: none"> • 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).

<p>roadsafety.transport.nsw.gov.au 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</p> <p>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.</p>	
<p>Information and Ticketing</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> • 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

	<ul style="list-style-type: none"> • Customer travel payment data
<p>Tolling</p> <p>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.</p>	<ul style="list-style-type: none"> • Account holder information for e-tag and tagless toll accounts • Vehicle and trip data collected from tolling cameras and e-Tag readers
<p>Compliance and Regulatory Services for roads and for maritime</p> <p>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.</p>	<ul style="list-style-type: none"> • 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

	<ul style="list-style-type: none"> • 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
<p>Transport Performance and Analytics</p> <p>TfNSW collects personal information by conducting surveys of the travel habits of the members of households which agree to participate in the survey.</p>	<ul style="list-style-type: none"> • Personal information for respondents of the annual Household Travel Survey
<p>Learning and Development</p> <p>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.</p>	<ul style="list-style-type: none"> • Information collected as a result of conducting training as a Registered Training Operator, including details such as: <ul style="list-style-type: none"> • 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.
Compliance Enforcement System (CES)	Records enforcement camera images and data
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

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 a NSW offence we can disclose that to the driver's home jurisdiction ¹
Service NSW	We can disclose any 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 <i>Passenger Transport Act 2014</i> 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 <i>Passenger Transport Act 2014</i> ⁶

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*

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
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

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*

¹¹ *Road Transport (Driver Licensing) Regulation 2017* clause 103

¹² ss. 75A(2B)-(2D) *Jury Act 1977*

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 <i>Heavy Vehicle National Law</i> (as a delegate of the National Heavy Vehicle Regulator) ¹⁸

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)*