Transport
State Transit

Privacy Management Plan

OCTOBER 2016 I Version 2

Contents

Date:	11 October 2016
Version:	2
Reference:	Privacy Management Plan
Review Date:	November 2017

1 Overview

1.1 Purpose

This Privacy Management Plan (**Plan**) has the following purposes, being to:

- meet the requirement to have such a plan under s 33 of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIPA**)
- demonstrate to members of the public how we meet our obligations under PPIPA and the *Health Records and Information Privacy Act 2002* (NSW) (**HRIPA**)
- provide staff with the necessary knowledge and skills to manage personal and health information appropriately and in accordance with the law
- enhance the transparency of our operations, and
- illustrate our commitment to respecting the privacy rights of our customers, clients, staff and members of the public.

1.2 Scope

This plan applies to our treatment of all personal and health information, whether it relates to a customer, an employee or another person (such as a contractor) ("**you**").

1.3 About Us

The State Transit Authority of New South Wales ("**State Transit**" and "**we**") is the government owned agency responsible for the operation of bus services across Sydney. Our functions are set out in Part 3, Division 2 of the *Transport Administration Act 1988.* For more information visit the State Transit website: www.statetransit.info.

1.4 Introduction to State Transit and its privacy context

State Transit is a 'public sector agency' for the purposes of PPIPA and HRIPA (*s 3(1) of PPIPA* and *s4(1) of HRIPA)*. We collect, hold, use and disclose your personal and health information for the purpose of carrying out our functions. We take your privacy seriously and will protect your personal and health information pursuant to PPIPA and HRIPA with reference to this plan.

PPIPA and HRIPA set out baseline privacy standards or 'privacy principles' which we must comply with. PPIPA covers personal information other than health information, and requires us to comply with 12 Information Protection Principles (*IPPs*). The IPPs cover the complete information life cycle from collection through to disposal. The IPPs include obligations with respect to data security, data quality and rights of access and amendment to one's own personal information, as well as how personal information may be collected, used and disclosed. There are also specific provisions in *Part 6 of PPIPA* for public registers.

Health information is regulated by a different set of principles set out in HRIPA. While health information is excluded from the definition of 'personal information' in PPIPA, it can be viewed as a type of personal information that relates to information about the physical or mental health of an individual or information provided or generated in the delivery of a health service. There are 15 Health Privacy Principles (*HPPs*) with which we must comply. Like the IPPs, the HPPs cover the entire information life cycle, but also include some additional principles with respect to anonymity, trans-border data flows,

linkage of health records and the use of unique identifiers.

There are exemptions to many of the privacy principles and public register provisions. Exemptions can be found in PPIPA and HRIPA, and in regulations, privacy codes of practice and public interest directions.

1.5 Privacy management across the Transport Agencies

Transport for NSW (**TfNSW**) provides coordinated planning and policy (including coordinating privacy matters) across Roads & Maritime Services, Sydney Trains, NSW Trains and State Transit.

At State Transit, privacy matters are managed by the General Counsel's Office.

1.6 Responsibilities of staff

State Transit must ensure that its staff are aware of their privacy responsibilities and are complying with our privacy policies, procedures, guidelines and standards, including this plan.

All of our staff are required to comply with PPIPA and HRIPA, including the IPPs and HPPs when handling personal and health information held by us. Both Acts contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information.

This plan aims to assist our staff to understand and comply with their obligations under both PPIPA and HRIPA.

State Transit staff should identify whether any of their new projects are likely to raise any privacy issues. The Information & Privacy Commission has developed a *checklist* to assist staff identify when there may be privacy issues early in a project's design stage. Please utilise the checklist and contact the General Counsel's office if need be.

2 Personal and health information held by us

2.1 What is personal information?

Personal information is defined in *s 4 of PPIPA*. In summary, personal information is information or an opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion.. It is not restricted to information that clearly identifies a person but may include information which leads to the identification of an individual when considered in association with other available information. Personal information can include a record which may contain your name, address and other details about you, your, bank account details, fingerprints, or a photograph or video. It can also include information that is recorded (for example, on paper or contained in a database) and also information that is not recorded (for example verbal conversations).

2.2 What does not constitute personal information?

Exclusions as to what constitutes personal information can be found at *ss 4(3)* and *4A of PPIPA*. There are 13 exclusions to the definition of personal information under PPIPA, including:

- 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, and
- information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Common examples of information falling within the exclusions include your own recruitment records, referee reports and performance appraisals, as well as information provided in the White Pages, a newspaper or a court judgment available on the internet. PPIPA also excludes from its sphere of operation certain information which may be held in connection with a number of activities authorised under a variety of legislation. For more information on these exclusions reference should be made to *ss 4(3)* and *4A of PPIPA* or contact made with the General Counsel's office.

2.3 What is health information?

Health information is defined in *s 6 of HRIPA*. Health information means:

- personal information that is also information or an opinion about:
  - a person's physical or mental health or disability;
  - a health service provided, or to be provided, to a person;
  - a person's express wishes about the future provision of health;
- other personal information collected to provide a health service;
- other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances; or
- genetic information that is or could be predictive of the health of a person or their relatives or descendants.

Exclusions as to what constitutes health information pursuant to HRIPA can be found at *s 5(3) of HRIPA*. There are 15 exclusions to the definition of health information under HRIPA. An example of information excluded by HRIPA is the results of a pre-employment medical check to assess a person's suitability to a job

which requires the person to drive a bus.

HRIPA also excludes from its sphere of operation certain information which may be held in connection with a number of activities authorised under a variety of legislation.

2.4 Main kinds of personal and health information held by us

State Transit collects and holds personal information and health information in order to provide an efficient, safe and reliable public transport service.

Personal information

Personal information collected by State Transit about employees and contractors may include, but is not limited to:

- personnel files
- membership of an Equal Employment Opportunity (EEO) group
- information held on the HR Information System database (e.g. address, salary details, birth date)
- payroll information (e.g. salary details, bank account details)
- disciplinary files
- leave applications
- investigation files (safety, grievance, fraud and/or corrupt conduct)
- accident/incident records and witness statements
- counselling files (including records of interview)
- information about secondary employment
- performance management and feedback records
- competency assessments and training records
- records of whether employees have taken a drug or alcohol test
- job applications
- images of individuals recorded on State Transit's CCTV surveillance system
- declared conflicts of interest.

Transport for NSW will also hold some of the above personal information as it provides human resources, payroll and records archival assistance to State Transit.

We may also collect:

- information about individuals obtained during the tender process
- information about individuals obtained in the course of developing and managing business relationships and maintaining contractual relationships
- information obtained in the course of complaint handling.

Health information

Health information collected by State Transit about employees and contractors may include but is not limited to:

- sick leave information such as leave applications, medical certificates;
- workers compensation files and claim forms;
- employee disclosures of pre-existing medical conditions
- urine drug analysis test results
- saliva drug analysis test results
- alcohol breath test results;
- records of attendance for Hepatistis B and Flu Shots and
- medical reports including pre-employment assessment of health, regular health monitoring (eg hearing, lung function), fitness for duty assessments, blood test results and change in health status reports.

The above information may be held by our medical and health care providers and if relevant to suitability for driving, Roads and Maritime Services.

Health information collected by State Transit about members of the public may include but is not limited to:

- medical information relating to personal injury claims; and
- information about members of an employee's household, e.g. as part of a claim for carer's leave.

2.5 Confidentiality of Records

Employees, contractors or consultants who collect, or have access to personal information or health information to enable them to perform their duties with State Transit must not access this information inappropriately nor disclose information without authorisation. Before being granted access to personal or health information, they may be asked to sign a confidentiality agreement.

Managers/supervisors are responsible for ensuring that:

- personal and health information retained in their area is managed in accordance with this plan;
- employees, contractors and consultants under their control sign a confidentiality agreement if they are required to access health information. Positions who must sign a confidentiality agreement include but are not limited to General Managers, Depot Managers, Service Managers and Health Services Officers;
- before an employee, contractor or consultant signs a confidentiality agreement, they must be provided a copy of this plan; and
- completed confidentiality agreements are retained on the Personnel file and noted in the HR Information System.

Employees, contractors or consultants who unintentionally receive access to personal or health information must maintain confidentiality of that information and must notify their direct manager that they received access to that information. Managers must ensure, where practicable, work processes are modified to prevent unintentional access being repeated.


BONDI JN
LIMITED STOPS
400
PLEASE
SIGNAL DRIVER
2602 ST
Opal
bus

3 How we manage personal and health information

We comply with the information protection principles and the health privacy principles summarised below.

4 Information Protection Principles and Health Privacy Principles

4.1 Limiting our collection of personal and health information – IPP 1 & HPP 1

We will only collect personal and health information (information) if:

- it is for a lawful purpose that is directly related to one of our functions or activities, and
- it is reasonably necessary for us to collect the information for that purpose.

We won't ask for your personal or health information unless it is directly related to our functions or activities and it's collection is reasonably necessary for us to perform those functions or activities.

4.2 How we collect personal and health information – source – IPP 2 & HPP 3

We will collect your personal or health information directly from you unless you have authorised otherwise or, in the case of health information, it would be unreasonable or impractical to obtain the information directly from you.

If we need your personal or health information, we will ask you directly for that information unless:

- you are under 16 years of age, we may instead collect personal information from your parent or guardian
- you have authorised collection of the information from someone else, in which case we may collect the information from that nominated person, and
- it would be unreasonable or impracticable to collect health information from you, in which case we may collect health information from another source. The Information & Privacy Commission's *Handbook to Health Privacy* provides some examples of when it might be unreasonable or impractical to collect health information directly from the person. Health information should be collected in accordance with these guidelines.

This principle is designed to limit the collection of your personal information without your knowledge. Secret or undisclosed collections may prevent you from exercising your rights.

4.3 How we collect personal and health information – IPP 4 & HPP 2

When collecting your information, we will:

- not collect excessive personal or health information
- not collect personal or health information in an unreasonably intrusive manner, and
- ensure that personal and health information collected is relevant, accurate, up-to-date and complete

We collect personal and health information in a variety of ways, including in writing, by email, through our website, over the phone, by fax, or in person. We will take reasonable steps to ensure that information we collect from you is not unreasonably intrusive or excessive, and is relevant, accurate, up-to-date and complete.

To determine what might be reasonable steps, we will consider:

- the purpose for which the information is being collected
- the sensitivity of the information
- how many people will have access to the information
- the importance of accuracy to the proposed use
- the potential effects for the individual concerned if the information is inaccurate, out-of-date or irrelevant
- the opportunities to subsequently correct the information, and
- the ease with which agencies can check the information.

Business units that collect information will implement procedures to ensure the information they hold is kept up to date and relevant. We mostly collect information through the use of forms which only contain relevant fields to ensure that we are not collecting excessive information.

4.4 Notification when collecting personal and health information – IPP 3 & HPP 4

When collecting your personal or health information, we will take reasonable steps to tell you:

- the fact that the information is being collected
- what it will be used for
- what other parties (if any) routinely receive this type of information from us
- whether the collection is required by law (and if so, which law) or is voluntary
- what the consequences will be if you do not provide the information to us
- your right to access and/ or correct your personal and health information held by us, and
- the name and contact details of the agency collecting and holding the information.

When collecting health information about you from a third party, we take reasonable steps to ensure that you are generally aware of the notification matters above.

Individuals providing their personal and health information to us have a right to know how their information will be used and disclosed. Notification allows a person to make an informed decision about whether they want to give their personal or health information to us. Notification is not required if the information is not collected directly from you, except in the case of health information. We are obliged when collecting health information to take reasonable steps to ensure that you are generally aware of the notification matters unless we are exempt because of circumstances described in the Information & Privacy

Commission's *Statutory Guidelines on the Collection of Health Information from a Third Party*.

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.

An example template privacy notice – for applications under the *Government Information (Public Access) Act 2009* (NSW) (GIPAA) – is attached in Annexure A to this plan. This template can be used as a guide to the types of matters to address in a privacy notice for any State Transit project, program or process in which personal or health information is collected. Any new project, program or process which might collect personal or health information should be reviewed by the Privacy Officer to ensure an adequate privacy notice has been prepared.

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

4.5 Retention and security – IPP 5 & HPP 5

We will take reasonable security safeguards to protect your personal and health information from loss, unauthorised access, use, modification or disclosure, and against all other misuse. We will ensure that your personal and health information is stored securely, not kept longer than necessary, and is disposed of appropriately. Where it is necessary for personal or health information to be transferred to a person in connection with the provision of a service to us, we will take steps to prevent unauthorised use and disclosure of that information.

Information security is fundamental to information privacy. Security measures include technical, physical and administrative actions.

State Transit's IT systems are designed to ensure that only authorised users can access them. Access controls are also employed to give access to information required for the user's particular role and functions.

The use of strong passwords by staff is enforced when using work computers, portable devices and email communications. Security software has been deployed across all network components, including the servers and network gateways. Security considerations are also taken into account in arrangements for data transmission (including encryption and password protection where appropriate), backup and storage.

State Transit also has comprehensive policies, procedures and processes in place to appropriately respond to any instance of unauthorised access to, use of or disclosure of personal and health information. For example, State Transit has an Information Security

Incident Management procedure which establishes an information security incident management process to ensure that security events (possible or potential breach or failure of safeguards) and security incidents are reported, investigated and properly managed. All State Transit employees are responsible for identifying and reporting events or issues with possible information security implications as quickly as possible. Prompt reporting enables prompt assessment, timely investigation and corrective action to be taken if necessary. Roles and accountabilities are detailed in the procedure.

We also have adequate firewall controls in place which help detect unauthorised access and use of our systems. For example, if data is accessed or changed without relevant access level authority (such as through password violation), this will be detected by the audit trail on the underlying databases detected through the application of our information security processes.

We also have a fraud control and corruption prevention strategy as part of our commitment to ensuring that our work environment is free of fraud and corruption. Where appropriate, instances of unauthorised access to, use of or disclosure of personal and health information will be notified to the NSW Police, the NSW Ombudsman, Information Commissioner or the NSW Auditor-General in accordance with our prevention strategy.

If an employee is responsible for a security breach, the matter will be investigated and the employee's manager will need to determine appropriate disciplinary action in consultation with our Workplace Relations Unit or the General Manager, People and Bus Systems.

Physical security is an important part of ensuring information is not inappropriately accessed. Our staff have access to secure storage spaces near their workstations to secure documents and devices which may contain personal or health information.

Keeping information for only as long as necessary is an effective way of reducing the risk that it may be mishandled. We follow best practice in records management for both electronic and paper records, and apply retention periods and disposal schedules in accordance with the *State Records Act 1998* (NSW). When no longer required, we destroy personal and health information in a secure manner as appropriate.

Where it is necessary for personal or health information to be transferred to a third party provider, such as Transport for NSW, 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 personal or health information that we hold. Transport for NSW is, for example, required to provide us with documented evidence that their obligations are being met. Their Audit and Risk Branch may review any aspect of their compliance and identify opportunities for improvements in performance and compliance. The next audit will be undertaken in 2017.

4.6 Transparency – IPP 6 & HPP 6

We will enable anyone to know, on request to the Privacy Officer:

- whether we are likely to hold their personal and health information
- the nature of their personal and health information
- the main purposes for which we use their personal and health information, and
- their entitlement to access their personal and health information.

We are required to be open about how we handle personal and health information. This is different to collection notification, which is more specific, and generally given at or before the time of collecting information.

The development and publication of this plan promotes accountability and increases the transparency of our information handling practices. The plan sets out the types of personal and health information we hold and explains our privacy obligations under the law, including the purposes for which we use the information and an individual's entitlement to access their information. Such a plan encourages openness and a proactive approach to privacy compliance.

This plan will be easily accessible on our website and available to download and print. For more information on our privacy practices, State Transit employees and contractors, and members of the public, can contact the Privacy Officer.

If you wish to know whether we hold your personal or health information, you should contact our Privacy Officer. If we do hold your personal or health information, our Privacy Officer can advise you of the nature of that information, the main purposes for which the information is used, and your right of access to that information.

4.7 Access – IPP 7 & HPP 7

We will allow people to access their personal and health information without excessive delay or expense. We will only refuse access where authorised by law, and we will provide written reasons, if requested.

Providing an individual access to their own information gives them the opportunity to find out what information we hold about them. We will let any individual see their own personal and health information in accordance with PPIPA and HRIPA, in many cases at no cost and through an informal request process.

We may at our discretion charge people for access to their health information provided that those charges are not excessive (i.e. they should be limited to recovery of our reasonable costs). We will not impose charges for the making of the access request but only for the provision of access. Where we decide to impose charges, we will seek the individual's agreement to those charges before providing access. Access to personal information under PPIPA is free of charge.

In relation to personnel records, access will depend on the file type. Any information pertaining to an individual's suitability for appointment of employment as a public sector official is not covered by PPIPA or HRIPA. Files about disciplinary matters and grievances are confidential and access is generally provided only to the staff member to whom the file relates. Establishment files, which hold information about the establishment of positions, may be viewed by staff at the discretion of a Human Resources staff member. Generally, staff may inspect files under supervision and will also be able to take photocopies of material on their file.

The Information & Privacy Commission's Best Practice Guide *Privacy and People with Decision-making Disabilities* explains how to provide access to information held about a person who has limited or no capacity.

4.8 Alteration – IPP 8 & HPP 8

We will allow you to update or amend your personal and health information, to ensure it is accurate, relevant, up-to-date, complete and not misleading. Where practicable, we will notify any other recipients of any changes.

Providing individuals with access to, and correction of, their information ensures individuals have control over their information by providing an opportunity to correct inaccurate, irrelevant and out-of-date information. We actively encourage you to help us keep any information we hold about you up-to-date, complete and accurate by contacting us with updated information. In some cases, you may be able to amend your own personal information by accessing an online account (for e.g. your Opal Account or MyPay account).

Once a request has been made to amend information, we must determine whether or not the personal or health information at issue is accurate, relevant, up-to-date, complete and not misleading. If the answer is 'no' then we must make appropriate amendments – whether by way of corrections, deletions or additions. When amending the information, we will have regard to the purpose for which the information was collected.

If the answer is 'yes' to the above question and the individual still insists on an amendment, we can decline to do so, but must allow the person to add a statement about the requested changes to our records. An example of a situation where it would be appropriate to attach a statement, instead of amending the information, would be a disputed medical diagnosis or a person with a criminal record maintaining their innocence.

Where practicable, we will also notify recipients of any amendments. We will consider the following factors when determining what is practicable:

- who the recipients of the information are
- the purpose for which the information was collected
- the sensitivity of the information
- the number of people who will have access to the information
- the importance of accuracy of the information
- the potential effects to the individual concerned if the information is inaccurate, out-of-date or irrelevant
- the ease of notifying recipients, and
- the costs of notifying recipients.

Requests for changes to personnel records will be processed by HR and in accordance with relevant policies.

If there is any doubt about whether a request for amendment of personal or health information is from the individual to whom the information relates (or their authorised representative), or if there is doubt about such a request, the request should be referred to the Privacy Officer.

4.9 Accuracy – IPP 9 & HPP 9

Before using personal or health information, we will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

We will take reasonable steps to ensure that personal and health information is still relevant and accurate before we use it. We ensure that information is recorded in a consistent format and attempt to confirm the accuracy of information collected from a third party or a public

source where practicable. We will not use personal or health information that we know is based on misleading or erroneous information.

We only need to take reasonable steps to check the information – although more steps will be needed if the use may disadvantage the person; for example, where the law enforcement exemption may apply. What might be considered 'reasonable steps' will depend upon the circumstances, but some factors to take into account are:

- the context in which the information was obtained
- the purpose for which we collected the information
- the purpose for which we now want to use the information
- the sensitivity of the information
- the number of people who will have access to the information
- the potential effects for the person if the information is inaccurate or irrelevant
- any opportunities we've already given the person to correct inaccuracies, and
- the effort and cost involved in checking the information.

4.10 Use – IPP 10 & HPP 10

We may use your personal and health information for:

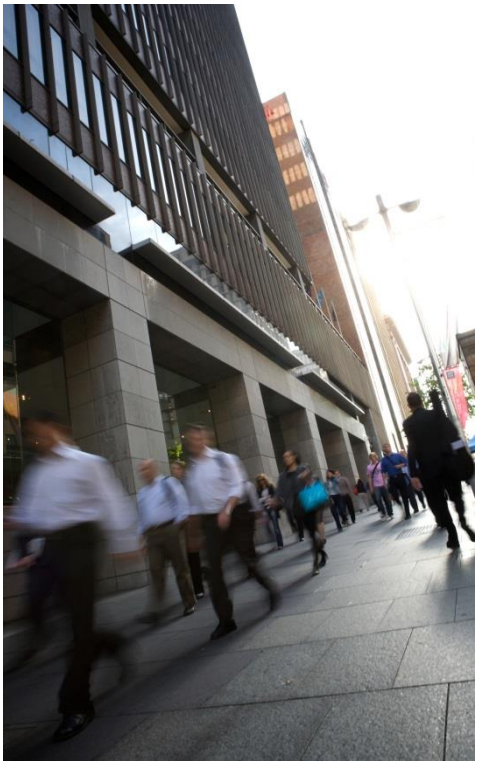
- the primary purpose for which it was collected
- a directly related secondary purpose
- another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health, or
- another purpose for which you have consented.

As a general principle, State Transit uses personal and health information that it collects for the purpose for which it was collected. The relevant purpose should have been set out in a privacy notice; see part 4.4 of this plan.

A directly related secondary purpose is a purpose that is very closely related to the purpose for collection and would be the type of purpose that people would quite reasonably expect their information to be used for. Examples of uses that are directly related to each other include quality assurance activities such as monitoring, evaluating and auditing.

Further to the circumstances set out above, we may also use health information to lessen or prevent a serious threat to public health or safety; management of health services; training; research purposes; finding a missing person; for law enforcement purposes and in respect of suspected unlawful activity, unsatisfactory professional conduct or breach of discipline.

The Information & Privacy Commission's Best Practice Guide *Privacy and People with Decision-making Disabilities* explains how to seek consent for a secondary use or disclosure of personal information from a person who has limited or no capacity. The Information & Privacy Commission's *Statutory Guidelines on Research* and *Statutory Guidelines on Training* explain how health information can be used or disclosed for research and training purposes.



4.11 Disclosure – IPPs 11 & 12 and HPPs 11 & 14

We may disclose your personal information if:

- the disclosure is directly related to the purpose for which the information was collected, and we have no reason to believe that you would object to the disclosure
- you have been made aware in the privacy notice that information of the kind in question is usually disclosed to the recipient and we are otherwise permitted under law to make such disclosure, or
- we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health.

Higher protections are afforded to sensitive personal information. We can generally only disclose sensitive personal information when the person has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health.

We can generally disclose health information when the person 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.

Most disclosures by State Transit in the course of performing its functions will not only be related to the primary purpose and within the individual's expectations but also explained in a privacy notice.

If we want to disclose information that is not covered by the exemptions, an individual can give us consent to disclose their personal or health information for a secondary purpose. PPIPA and HRIPA both allow an 'authorised person' to consent on behalf of the individual concerned.

Disclosure of personal information for any other purpose needs to be tested against the exemptions outlined below. Disclosures of health information should be tested against the exemptions outlined in *Schedule 1 of HRIPA*. Before disclosing personal or health information for any other purpose, staff should check with the Privacy Officer. Requests for personal or health information from outside bodies, including from government agencies, should be referred to the Privacy Officer to assess whether an exemption applies.

The Information & Privacy Commission's Best Practice Guide *Privacy and People with Decision-making Disabilities* explains how to seek consent for a secondary use or disclosure of personal information from a person who has limited or no capacity. The Information & Privacy Commission's *Statutory Guidelines on Research* and *Statutory Guidelines on Training* explain how health information can be used or disclosed for research and training purposes.

Trans-border disclosure of health information

We can only transfer health information outside NSW if one of the following applies:

- the individual concerned has consented
- if it is necessary for a contract with (or in the interests of) the person concerned
- if it will benefit the person concerned and it is impracticable to obtain their consent but we believe the person would be likely to give their consent
- we reasonably believe that the recipient of the information is subject to a law or binding scheme equivalent to the HPPs
- we have bound the recipient by contract to privacy obligations equivalent to the HPPs, or
- if it is permitted or required by legislation or any other law.

We can, however, disclose health information (whether within or outside NSW) to prevent a serious and imminent threat to life, health or safety of an individual or a serious threat to public health or safety.

Trans-border disclosure of personal information

We must not disclose personal information to any person or body in a jurisdiction outside NSW or to a Commonwealth agency unless:

- a relevant privacy law that applies to personal information concerned is in force in that jurisdiction, or
- the disclosure is permitted under a privacy code of practice.

Before making a transborder disclosure, we will make the assessment required by section 19(2)(a) and HPP 14. These require a disclosing agency to be satisfied that the privacy protections substantially similar to those in NSW operate in the destination jurisdiction.

4.12 Identifiers – HPP 12

We will only identify individuals by using unique identifiers if it is reasonably necessary for us to carry out our functions.

We will ensure that we only assign unique identifiers to individuals in

relation to their health information if it is reasonably necessary for us to carry out our functions efficiently.

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 e.g. a customer number, unique patient number, tax file number or driver's license number). Identifiers will be perceived as health information and subject to HRIPA.

4.13 Linkage of Health Records – HPP 15

We only use health records linkage systems if an individual has provided or expressed their consent, unless the linkage is for research purposes and has been approved in accordance with statutory guidelines.

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*.

Exemptions

PPIPA and HRIPA provide that we need not comply with some or all of the IPPs or HPPs if certain circumstances apply.

Some examples of exemptions most relevant to our functions and activities include:

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- use or disclosure for law enforcement purposes or investigative functions
- where another law authorises or requires us not to comply
- where non-compliance is lawfully authorised or required
- where compliance would prejudice the individual
- when we exchange information with other public sector agencies
- some research purposes

If an exemption applies to a particular situation, we will inform the individual(s) concerned about the exemption and why it applies, as is reasonable and appropriate in the circumstances.

4.14 Privacy codes of practice

PPIPA and HRIPA permit the development of privacy codes of practice by an agency which may modify the application of an IPP, HPP or public register provision. A code may exempt an agency from the requirement to comply with any or all of the privacy principles, or specify the manner in which the privacy principles are to be applied or followed by an agency in certain circumstances.

At the time of this plan's publication, a privacy code of practice or health privacy code of practice has not been developed by and approved for State Transit.

4.15 Directions by the Privacy Commissioner

PPIPA and HRIPA allow the Privacy Commissioner to make directions that exempt agencies from complying with an IPP, HPP, privacy code of practice or health privacy code of practice. Directions could also be given to modify the application of an IPP, HPP, privacy code of practice or health privacy code of practice.

On 1 January 2016, additional exemptions were inserted into PPIPA. These include exemptions relating to:

- investigative functions of agencies
- information exchanges between public sector agencies
- research
- credit information

These exemptions were previously Public Interest Directions made by the Privacy Commissioner under *s 41 of PPIPA*.

4.16 Memoranda of Understanding

State Transit has a limited number of Memoranda of Understanding (**MOUs**) with Transport for NSW's Transport Shared Services for access to State Transit information. These MoUs cover functions involving State Transit employees including recruitment, employee services, payroll and workers compensation claims. State Transit does not have any MoUs covering access to customer information. These MOUs provide assurance that information obtained from State Transit is accessed, stored, maintained and disclosed for an agreed purpose within the terms of the agreement.

4.17 Public registers

Part 6 of PPIPA prescribes special rules for personal and health information held on public registers, which is a register of personal or health information that is required by law to be, or is made, publicly available or open to public inspection, whether or not on payment of a fee.

Such rules regulate when we can disclose personal or health information contained in a public register, and when an individual can ask for their personal or health information to be suppressed from a public register.

We do not maintain any public registers for the purposes of PPIPA or HRIPA.

4.18 Offences

Both PPIPA and HRIPA contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information.

A table has been provided below for ease of reference. It is also an offence under section 308H of the Crimes Act to access or modify restricted computerised records for purposes that are not connected with the duties of a person. The maximum penalty is 2 years.

Offence	Maximum penalty	Legislative provision
It is a criminal offence for a public sector official to corruptly disclose and use personal or health information.	Fine of up to 100 penalty units ($11,000) or imprisonment for two years, or both.	s 62 of PPIPA and s 68 of HRIPA.
It is a criminal offence for a person to offer to supply personal or health information that has been disclosed unlawfully.	Fine of up to 100 penalty units ($11,000) or imprisonment for two years, or both.	s 63 of PPIPA and s 69 of HRIPA.
It is a criminal offence for a person – by threat, intimidation or misrepresentation – to persuade or attempt to persuade an individual: • to refrain from making or pursuing a request to access health information, a complaint to the Privacy Commissioner or the NSW Civil and Administrative Tribunal, or an application for an internal review; or • to withdraw such a request, complaint or application.	Fine of up to 100 penalty units ($11,000).	s 70(1) of HRIPA.
A person must not – by threat, intimidation or misrepresentation – require another person to give consent under HRIPA, or require a person to do, without consent, an act for which consent is required.	Fine of up to 100 penalty units ($11,000).	s 70(2) of HRIPA
It is a criminal offence for a person to: • wilfully obstruct, hinder or resist the Privacy Commissioner or a member of the staff of the Privacy Commissioner • refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner, or • wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of the staff of the Privacy Commissioner • in the exercise of their functions under PPIPA or any other Act.	Fine of up to 10 penalty units ($1100).	s 68(1) of PPIPA.

5 Privacy and other legislation relating to personal and health information

5.1 Privacy legislation

- *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA)
- *Health Records and Information Privacy Act 2002* (NSW) (HRIPA)
- *Privacy and Personal Information Protection Regulation 2005* (NSW)
- *Health Records and Information Privacy Regulation 2012* (NSW)
- Privacy Codes of Practice, Directions and Statutory Guidelines made under PPIPA and HRIPA

5.2 Other relevant legislation

Other legislation that may also affect the application of the privacy principles to State Transit includes, but is not limited to, the following:

- *Transport Administration Act 1988* (NSW)
- *Passenger Transport Act 1990 (NSW)*
- *Criminal Records Act 1991* (NSW)
- *Government Information (Public Access) Act 2009* (NSW)
- *State Records Act 1998* (NSW)
- *Workplace Surveillance Act 2005* (NSW)
- *Surveillance Devices Act 2007* (NSW)
- *Ombudsman Act 1974* (NSW)
- *Public Interest Disclosures Act 1994* (NSW)
- *Telecommunications (Interception and Access) Act 1979* (Cth)
- *Workers Compensation Act 1987 (NSW)*
- *Workers Compensation and Workplace Injury Management Act 1998 (NSW)*

We encourage people to apply for access for information about themselves under PPIPA or HRIPA which do not require payment of an application fee unlike applications under the Government Information (Public Access) Act 2009.

We note that subpoenas or warrants, issued by a court or a magistrate may require us to release personal and health information.

6 How to access and amend personal and health information held by us

6.1 Request to access and amend

We encourage you to contact the member of staff or unit holding your information if you wish to access or amend your personal or health information. In some cases, you may be able to access and amend your own personal information by accessing an online account (for e.g. your Opal Account or MyPay account).

If you do not know which unit to contact regarding your request or your request has been denied, you may request access to and/ or alteration of your personal or health information from the TfNSW Information & Privacy Unit by email or post to:

Email: *privacy@transport.nsw.gov.au*

Mail: The Privacy Officer
Transport for NSW
PO Box K659
Haymarket NSW 1240

Your request should:

- include your name and contact details state whether you are making the application under PPIPA (personal information) or HRIPA (health information)
- explain what personal or health information you want to access or amend, and
- explain how you want to access or amend it.

Application forms have been developed to assist you with your request. A copy of the application forms can be found at *www. transport.nsw.gov.au/aboutus/ privacy* The application forms can also be found on our website.

If State Transit staff want to access and/or amend their personnel file, a request may be made to Transport Shared Services. Please contact HR Advisory on 1800 618 445 or at tfnswhr@transport.nsw.gov.au for more details.

7 Privacy complaints and internal review

A person who wishes to make a complaint in relation to privacy may:

- resolve the matter informally
- follow the general complaint process by contacting 131 500 or filling out a form on the TfNSW *website*
- contact the Privacy Commissioner
- apply for an internal review.

7.1 Resolving the matter informally

We encourage people to try to resolve privacy concerns with us informally or at least contact the General Counsel's office to discuss the issue, before lodging an application for internal review.

Post: General Counsel's Office
State Transit Authority
GPO Box 2557
Strawberry Hills NSW 2012

Phone: 02 9245 5760

Email: *privacy@sta.nsw.gov.au*

7.2 How to apply for an internal review of conduct

A person who is aggrieved by the conduct of State Transit in relation to personal or health information is entitled to an internal review of that conduct by us. An internal review is the process by which we manage formal, written privacy complaints.

TfNSW centrally processes all requests for internal reviews made to the Transport Agencies including State Transit. You may apply in writing for an internal review by sending your request to the TfNSW Information & Privacy Unit:

Email: *privacy@transport.nsw.gov.au*

Mail: The Privacy Officer
Transport for NSW
PO Box K659
Haymarket NSW 1240

7.3 Internal review process

The Transport Agency nominated on your application will make the decision on your request and will liaise with you about your application. TfNSW will acknowledge receipt of an internal review within **5 working days** and the Transport Agency responsible for the internal review will aim to:

- complete the internal review within **60 calendar days**, and
- respond to the complainant in writing within **14 calendar days** of determining an internal review.

Contact will be made to advise how long the review is likely to take, particularly if it may take longer than expected.

An application for internal review must:

- be in writing
- be sent to TfNSW
- specify an address in Australia to which the applicant is to be notified after the completion of the review, and
- be lodged at TfNSW within six months from the time the applicant first became aware of the conduct that they want reviewed.

An application form has been developed to assist individuals wishing to apply for an internal review. A copy of the application form can be found at http://www.transport.nsw.gov.au/aboutus/ privacy. The application form can also be found on our website. An application for internal review can be made on behalf of someone else. Where the applicant is not literate in

both English and their first language and where there is no other organisation making the application on their behalf, staff should help the person to write their application. Staff should use a professional interpreter, if necessary. Applications in other languages will be accepted and translated, and all acknowledgements and correspondence to the applicant will be translated.

If the complaint is about an alleged breach of the IPPs, HPPs, privacy code of practice or health privacy code of practice, the internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is an employee or an officer of the agency, and
- is qualified to deal with the subject matter of the complaint.

State Transit will keep the Privacy Commissioner informed of the progress of the internal review.

7.4 Extensions of time lodgement of applications for internal review

While PPIPA allows applicants six months to apply for an internal review from the time the applicant first becomes aware of the conduct, State Transit may accept late applications. Possible acceptable reasons for delay may be:

- the applicant's ill-health or other reasons relating to capacity; or
- the applicant reasonably believing that he or she would suffer ill-effects as a result of making an application at earlier time.

Some late applications may not be accepted if they cannot be investigated in a meaningful way. Final decisions on the acceptance of late applications will only be made by the General Counsel's office. Where the decision is made not to accept an application because of the lapse of time since the incident, the reason will be explained in a letter to the applicant.

7.5 Privacy Commissioner

You may make a privacy complaint directly to the Privacy Commissioner if you believe that we have breached an IPP, HPP, privacy code of practice or health privacy code of practice that applies to us.

When the Privacy Commissioner accepts a complaint about the conduct of a public sector agency, it usually attempts to resolve it through:

- conciliation - this is final and completes the process, or
- preparation of a report on findings and recommendations. This report is not binding on the public sector agency, in other words it has only persuasive influence.

If the Privacy Commissioner's intervention does not resolve the matter to the complainant's satisfaction, the complainant does not have a right to litigate their complaint in the NSW Civil and Administrative Tribunal (**Tribunal**) and obtain a binding decision.

For more information on how the Privacy Commissioner handles privacy complaints received from members of the public, please refer to the Information & Privacy Commission's *Protocol for Handling Privacy Complaints*. The Privacy Commissioner can be contacted as follows:

Office: Information and Privacy Commission NSW
Level 3, 47 Bridge Street
Sydney NSW 2000

Post: PO Box R232, Royal Exchange NSW 1225

Phone: 1800 472 679

Fax: 02 8114 3756

Email: *ipcinfo@ipc.nsw.gov.au*

7.6 External review by the NSW Civil and Administrative Tribunal

Individuals can seek an external review by the Tribunal if they are not satisfied with the outcome of an internal review. Individuals can also seek an external review if they do not receive an outcome of the review within 60 days.

To seek an external review, a person must apply to the Tribunal within 28 days from the date of the internal review decision.

NCAT may order the agency to change its practices, apologise or take steps to remedy any damage. NCAT's decision is enforceable and it may award compensation.

For more information about seeking an external review including current forms and fees, please contact the Tribunal.

Office: NSW Civil and Administrative Tribunal (NCAT)
Administrative and Equal Opportunity Division
Level 10, John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000

Phone: 1300 006 228 or 02 9377 5859 (TTY)

Fax: 02 9377 5723

Website: *www.ncat.nsw.gov.au*

8 Promoting Privacy

8.1 Policies and procedures

Our policies and procedures on managing information reflect the requirements of applicable legislation, NSW government policy and guidelines and appropriate Australian Standards.

We have a number of policies and procedures which have been prepared to inform and assist staff in protecting privacy. Any policies or procedures that may impact on the management of personal or health information are reviewed to ensure that they comply with PPIPA and HRIPA. They include:

- Code of Conduct
- Fraud Control and Corruption Prevention Policy
- Video Surveillance Policy
- Alcohol and Other Drugs Policy
- Electronic Information Privacy Policy.

TfNSW has also identified a need to draft a number of policies and procedures for the Transport Agencies to provide a consistent structure for the management of personal and health information, and to ensure compliance with PPIPA and HRIPA. We have made it a priority to implement such policies and procedures in consultation with TfNSW.

8.2 Dissemination of the plan, policies and procedures

Policies and procedures, including this plan, are communicated to staff in a range of ways, including through the State Transit intranet, printed copies and training. The Code of Conduct specifically refers to the importance of protecting privacy and complying with PPIPA and HRIPA.

All policies and procedures are sourced, numbered, dated and owned by a specific management position, and are systematically reviewed and updated when necessary.

Any new policy or procedure, or any policy that is changed or updated, is undertaken in consultation with relevant business areas and receives the endorsement of senior management staff, including the Privacy Officer, General Counsel and the Chief Executive. Our staff are advised of new or updated policies and procedures through the intranet and, on occasion, targeted training.

We will ensure that staff will be notified of this plan and will have easy access to a copy of the plan on our website and intranet. Any unauthorised access to, use of and disclosure of personal and health information will be managed in the manner set out in paragraph 4.5 above.

State Transit educates members of the public about its privacy obligations and the public's privacy rights through:

- the publication of this plan on our website
- publishing privacy policies such as the State Transit User Privacy Policy, and
- providing notices under s 10 of PPIPA.

9 Annexure A

Example privacy notice under PPIPA on a GIPA application form

State Transit must comply with the privacy principles set out in the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA).

Personal information provided on this form is collected and held by State Transit for the purposes of processing your request for information under the *Government Information (Public Access) Act 2009* (NSW). State Transit will only use your personal information for this purpose.

State Transit may disclose your personal information to assess your application or to verify it. Otherwise we will not disclose your personal information without your consent unless required or authorised by law.

The provision of your personal information is voluntary. Personal information not relevant to this request for information should not be included on this application form. Please note that we may refuse access to the information requested if you do not provide proof of identity.

Your personal information will be held by State Transit at 15 Bourke Road, Mascot, NSW 2020. Individuals generally have the right of access to and correction of their personal and/or health information held by State Transit. Should you wish to access or amend your information held by us, please contact us by writing to:

State Transit Authority
Customer Relations
PO Box 2557
Strawberry Hills NSW 2012.