Privacy Management Plan

1 Introduction

1.1 Purpose

This Privacy Management Plan (the plan) explains how Sydney Motorway Corporation Pty Limited and its subsidiaries (collectively referred to as SMC) manage personal and health information under NSW privacy laws.

SMC takes its responsibilities to protect the privacy rights of stakeholders, staff and members of the public seriously.

Through this plan, SMC:

- illustrates our commitment to respecting the privacy rights of members of the public, contractors and staff and enhances the transparency of our operations
- provides our staff and contractors with the necessary knowledge and skills to manage personal and health information appropriately
- meets the requirement for us to have such a plan under s 33 of the PPIP Act.

1.2 Scope

This plan applies to our treatment of all personal and health information, whether it relates to a stakeholder, a staff member or another person (such as a contractor).

The plan applies to all permanent, temporary and casual staff employed by SMC and to skill hire, contractors and consultants engaged by SMC (collectively referred to as SMC staff).

1.3 About us

SMC is a *Corporations Act 2001 (Cth)* entity with a majority independent board that is wholly owned by the NSW Government, with the Treasurer and Minister for Roads, Maritime and Freight as joint shareholders.

SMC finances, delivers, operates and maintains major infrastructure solutions to support Sydney's long-term economic growth and high quality transport connections for anticipated population growth.

SMC is currently delivering the WestConnex motorway, Australia's largest transport infrastructure project, on behalf of the NSW Government.

Roads and Maritime Services (RMS) has commissioned SMC to deliver WestConnex on behalf of the NSW Government. RMS and SMC are working together to manage the project planning processes.

Core responsibilities of SMC:

- Procuring and managing contracts relating to the development, construction, funding, operation and maintenance of WestConnex;
- Developing and making recommendations on scope, staging and any other matter in connection to the WestConnex scope of works;
- Preparing planning approval requests, management of environmental assessments and related community consultation for each stage;
- Administrating agreements relating to the development, construction, funding, operation and maintenance of WestConnex.

Further information about our structure and functions is available at www.sydneymotorway.com.au.

We collect, hold, use and disclose personal and health information for the purpose of carrying out these functions.

1.4 Information and health protection principles

Both the PPIP Act and HRIP Act contain principles about managing personal and health information, which we must comply with. These principles are legal obligations that describe what we must do when we collect, store, use or disclose personal and health information.

The PPIP Act sets out how we must manage personal information, and requires us to comply with 12 Information Protection Principles (IPPs). The HRIP Act sets out how we must manage health information, and requires us to comply with 15 Health Privacy Principles (HPPs).

We explain how we manage personal and health information in Part 3.

1.5 What is personal information?

Personal information is defined in s4 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 a person's name, bank account details, fingerprints, or a photograph or video.

1.5.1 What is *not* personal information?

There are certain types of information that are not considered personal information and these are outlined at ss4(3) and 4A of the PPIP Act.

This means that the IPPs do not apply to our handling of certain types of information. 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 a court judgment available on the internet).

1.6 What is health information?

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

- personal information that is also 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 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
- genetic information that is or could be predictive of the health of a person or their relatives or descendants
- healthcare identifiers.

1.6.1 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 s 5(3) of the HRIP Act and include some of the types of information listed in Part 1.5.1.

For example, the results of a pre-employment medical check to assess a person's suitability to a job, which requires the person to drive a particular vehicle is not considered health information.

2 Personal and health information held by us

2.1 Types of personal and health information held by us

In order to conduct its business operations, SMC collects personal information about SMC staff and stakeholders. This information is held in a number of different locations and formats.

Some examples of the types of personal and health information we hold about our staff include:

- personal contact details and emergency contact details (including telephone number, postal and email address)
- date of birth
- financial information (such as salary, bank account information, tax file number)
- personnel information (such as attendance records, leave balances, educational and professional qualifications, training records)
- health information (including medical certificates, reports and files, and fitness for duty assessments)
- statements and opinions
- photographs/footage
- injury management information such as workplace injuries, workers' compensation claims and payments and return to work plans.

Some examples of the types of personal and health information we hold about our stakeholders and members of the public include:

- name and personal contact details (including telephone number, postal and email address)
- general enquiries, feedback and complaints
- health information (including requests for counselling services)
- photographs/footage (from on-site CCTV).

We do not maintain any public registers for the purposes of the PPIP Act or the HRIP Act.

3 How we manage personal and health information

3.1 Introduction

This section provides an overview of how we comply with the IPPs and HPPs when we handle the personal and health information of our stakeholders, staff and members of the public.

3.2 Collection

3.2.1 Collection for lawful purposes (IPP 1 & HPP 1)

We will only collect personal and health information if:

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

We collect personal and health information in a variety of ways, including in writing, by email, through our website, over the phone, by fax, recordings (such as CCTV footage) or in person.

We only ask for personal and health information that is reasonably necessary to the task at hand and is required for our functions as outlined in Part 1.3. For example, SMC may collect personal information about you for the following purposes:

- to deal with specific inquiries or issues that you have raised with SMC or its service providers
- to provide information to you about the WestConnex project (including by way of direct mail, email, SMS and MMS). You always have the right to opt-out of receiving such information. You may exercise that right at any time by contacting SMC as set out in Section 6 below;
- in relation to any employment application you may make to SMC in order to assess your suitability for

employment;
- other purposes which SMC identifies to you at the time of collection of the information (or as soon as practicable after collection).

We avoid collecting sensitive personal information if we don't need it. Sensitive information is information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

3.2.2 Direct collection (IPP 2 & HPP 3)

We generally collect personal or health information directly from the person concerned, for example when it is provided by the individual:

- Directly to SMC
- directly to SMC contractors
- through the WestConnex website
- at a community engagement forum
- through website technologies such as cookies, internet tags or web beacons and navigational data collection.

We will only collect information from a third party where:

- the person has authorised collection of the information from someone else (eg. from a person's treating doctor regarding a workers' compensation claim)
- the person is under 16 years of age – in which case we may instead collect personal information from the person's parent or guardian
- in the case of health information, it would be unreasonable or impracticable to collect information from an individual.

3.2.3 Requirements when collecting information (IPP 3 & HPP 4)

When collecting personal or health information from an individual, we take reasonable steps to tell them:

- the fact that the information is being collected
- what it will be used for
- what other parties (if any) we may share the information with
- of any law that requires that particular information to be collected
- what the consequences will be for the person if they do not provide the information to us
- that they have a right to access and/or correct their personal and health information held by us, and
- the name and contact details of the organisation collecting and holding the information.

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

Generally, we provide this notification by way of a 'privacy notice' that is included on an application form, web page, or in a verbal notice at the time the personal or health information is collected, or as soon as we can afterwards.

3.2.4 Relevant (IPP 4 & HPP 2)

When collecting information from an individual, 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 take reasonable steps to ensure that information we collect from an individual is not unreasonably intrusive or excessive, and is relevant, accurate, up-to-date and complete.

To determine what might be reasonable steps, we consider:

- the purpose for which the information was 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, and
- the opportunities to subsequently correct the information.

3.3 Retention and security (IPP 5 & HPP 5)

We will take reasonable security safeguards to protect personal and health information from loss, unauthorised access, use, modification or disclosure, and against all other misuse. We will ensure personal and health information is stored securely, not kept longer than necessary, and 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.

We consider the security of the personal and health information that we hold fundamental to protecting privacy.

Information is stored in a variety of ways, including across all of our sites, systems, and secure off site repositories in paper and digital formats.

We maintain reasonable security measures, including technical, physical and administrative actions, to protect information from unauthorised access and misuse.

Examples of such security measures 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
- implementing and maintaining strong security software across all network components in arrangements for data transmission (including encryption and password protection where appropriate), backup and storage
- maintaining logs and audit trails which are monitored and retained on a regular basis
- providing staff with access to secure storage spaces near workstations to secure documents and devices
- physically securing sensitive and confidential information in locked rooms
- maintaining and continually improving information security management systems that comply to ISO/IEC 27001:2013 standard
- 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 staff.

3.4 Accuracy and access

3.4.1 Transparency (IPP 6 & HPP 6)

We enable anyone to know:

- whether we are likely to hold their personal and health information
- the nature of the 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.

Often we rely on the person providing the information to confirm its accuracy. Sometimes we will independently verify the information (for example to confirm the details of a complaint).

3.4.2 Access to personal and health information (IPP 7 & HPP 7)

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

Members of the public

We encourage you to contact the staff member or business unit holding your information if you wish to access it. If you are unsure about who to contact, please contact us on the details included at Part 6.

Staff

Staff are able to access their personnel file by making a request to Human Resources at hr.enquiries@westconnex.com.au

Files about disciplinary matters and grievances are confidential and access is generally provided only to the staff member to whom the file relates. Generally, staff may view files under supervision.

3.4.3 Alterations to personal and health information (IPP 8 & HPP 8)

We will allow people to update or amend their 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.

We encourage you to help us keep any information we hold about you accurate, up-to-date and complete by contacting us with updated information.

If information we hold is accurate, relevant, up-to-date, complete and not misleading but a person 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. For example, it may be appropriate to attach a statement, instead of amending the information, for a disputed medical diagnosis or a person with a criminal record maintaining their innocence.

Members of the public

We encourage you to contact the staff member or business unit holding your information if you wish to access it. If you are unsure about who to contact, please contact us on the details included at Section 6.

Staff

In some cases, staff employed by SMC can amend their own personal information by accessing the ADP Employee Self Service online system at www.myadppayroll.com.au. Contractors engaged by SMC through a third party may update their personal details directly with their employer.

Staff are able to request amendment of their personal or health information by contacting Human Resources and Services at hr.enquiries@westconnex.com.au.

We encourage you to keep your personal 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.

3.5 Use

3.5.1 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.

3.5.2 Limited Use (IPP 10 & HPP 10)

We may use 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
- another purpose for which the person has consented, or
- another purpose where permitted by law.

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

Generally, we only use personal and health information for the purpose for which is was collected. That purpose is set out in the privacy notice on the WestConnex and SMC websites.

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.

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 staff
- unsatisfactory professional conduct or breach of discipline
- finding a missing person
- preventing a serious threat to public health and safety.

3.6 Disclosure

3.6.1 Disclosure (IPPs 11 & 12 and HPPs 11 & 14)

We may disclose 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 the individual concerned would object to the disclosure
- the individual has been made aware in the privacy notice that information of the kind in question is usually disclosed to the recipient
- 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.

SMC works in partnership to carry out its business operations and deliver its projects. It is sometimes necessary for information to be passed to our industry partners, contractors or a NSW Government agency in order for us to ensure the best response possible to enquiries and complaints.

The persons to whom SMC may disclose your personal information to include:

- specified persons in accordance with a request made by you
- service providers of SMC
- RMS and other Government agencies
- your authorised representatives or legal advisors
- SMC's professional advisors, and
- any other person that would be reasonably expected.

Higher protections are afforded to 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 such 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.

When we disclose information, it means that we give it to a third party outside of SMC to use the information for their own purposes. We will only do this in the circumstances outlined above, or when you have provided consent for us to do so or it is permitted or required to by law.

3.6.2 Identifiers (HPP 12)

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

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).

3.7 Exemptions to how we manage personal and health information

3.7.1 Specific exemptions contained in the PPIP Act and the HRIP Act

The PPIP Act and HRIP Act provide that we need not comply with some or all of the IPPs and HPPs if certain circumstances apply.

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

- unsolicited information
- 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
- 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.

3.7.2 Other legislation

The following legislation may affect how the IPPs and HPPs apply to us:

- Criminal Records Act 1991 (NSW)
- State Records Act 1998 (NSW)
- Workplace Surveillance Act 2005 (NSW)
- Surveillance Devices Act 2007 (NSW)
- Ombudsman Act 1974 (NSW)
- Telecommunications (Interception and Access) Act 1979 (Cth)
- Workers Compensation Act 1987 (NSW).

3.8 Offences

Both the PPIP Act and HRIP Act contain criminal offence provisions applicable to persons who misuse personal and health information.

Our 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.

4 Strategies for compliance and best practice

4.1 Introduction

We are committed to protecting the privacy rights of members of the public, stakeholders and staff. We adopt several strategies to implement best practice principles and comply with our obligations under the PPIP Act and HRIP Act that recognise that privacy is a shared responsibility within the organisation.

4.2 Policies and procedures

In addition to this plan, we have developed a number of policies and guidelines to inform and assist staff in protecting privacy. These policies provide best practice guidance and practical advice on matters relating to:

- acceptable use of technology
- dealing with confidential information
- information security
- records management
- privacy breaches
- use of social media

Our 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 intranet.

We regularly review and update our policies and procedures as necessary. For example, to reflect amendments to the PPIP Act or HRIP Act so our staff and members of the public receive accurate information about our privacy practices.

Any new policy or procedure, or any policy that is significantly changed or updated, is developed in consultation with relevant business areas and receives the endorsement of senior management and the Chief Executive Officer, before being circulated to staff.

Policies and procedures, including this plan, are communicated to staff in a range of ways, including through our intranet, staff newsletters, induction of new staff and on-the-job training. Information about our privacy practices are also made available on our dedicated privacy page on our website.

4.3 Promoting privacy awareness

We undertake a range of initiatives to ensure our staff and members of the public are informed of our privacy practices and obligations under the PPIP Act or HRIP Act. This also assists in identifying and mitigating risks associated with privacy and encourages best practice.

We promote privacy awareness and compliance by:

- publishing and promoting this plan on our intranet and website
- including mandatory privacy training in our induction program (for example, through the Code of Conduct)
- publishing and promoting all 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
- participating annually in Privacy Awareness Week (which includes reminding all staff of their privacy rights and obligations during this period)
- delivering 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
- 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).

4.4 Review and continuous improvement

We are committed to identifying opportunities for improvement and better practice in protecting the privacy of our stakeholders, staff and members of the public.

We consistently evaluate the effectiveness and appropriateness of our privacy practices, policies and procedures to ensure they remain effective and identify, evaluate and mitigate risks of potential non-compliance.

We are committed to:

- monitoring and reviewing our privacy processes regularly
- further promoting and maintaining privacy awareness and compliance
- actively participating in Privacy Awareness Week
- actively promoting information security awareness to ensure all staff fully understand their responsibilities of information security compliance in their day-to-day activities.

5 If you think we have breached your privacy

We encourage you to contact us directly to resolve any concerns you have about our handling of your personal or health information.

If you think we have breached your privacy, we encourage you to discuss any concerns with the staff member or business unit dealing with your information, or contact us on the details provided in Part 6.

5.1 Your right of internal review

You have the right to ask us for an internal review if you think we have breached your privacy.

An application for internal review must:

- be in writing
- be addressed to SMC
- specify an address in Australia to which you can be notified after the completion of the review.

To apply for an internal review into a privacy issue, you can submit a request, including any relevant material, by email or post to us at the details provided in Part 6.

5.1.1 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 SMC, 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.

We are required to give a copy of your internal review request to the Privacy Commissioner. We will also send a copy of the draft internal review report to the Privacy Commissioner and we must take into account any submissions made by the Privacy Commissioner. We will keep the Privacy Commissioner informed of the progress of the internal review and will provide a copy of the finalised internal review report.

5.1.2 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.

We may accept late applications in certain circumstances (such as if you have only become aware of your right to seek an internal review or for reasons relating to your capacity to lodge an application on time). If we do not accept your application, we will provide our reasons in writing.

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

- complete the internal review within 60 calendar days, and
- respond to you in writing within 14 calendar days of completing the internal review.

We will contact you to advise how long the review is likely to take, particularly if it may take longer than expected.

If the internal review is not completed within 60 days, you have a right to seek a review of the conduct by the NSW Civil and Administrative Tribunal (see below).

5.2 Your right to external review

You have the right to apply to the NSW Civil and Administrative Tribunal if you have sought an internal review and:

- you are not satisfied with the outcome of the internal review
- you are not satisfied with the action taken in relation to your application for internal review
- you do not receive an outcome of the internal review within 60 days.

For more information about seeking an external review, contact the Tribunal on the details below:

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

Website: www.ncat.nsw.gov.au

5.3 Complaints to the Privacy Commissioner

You 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: 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

6 Contact Us

For further information about this plan or questions about your privacy, please contact us on the details below.

Post: Privacy Officer
Sydney Motorway Corporation
GPO Box 3905
Sydney NSW 2001

Phone: 1800 660 248

Email: privacy@westconnex.com.au

Web: www.westconnex.com.au or www.sydneymotorway.com.au