Service NSW Privacy Management Plan

Date: 28 October 2014

Document Information

Title	Privacy Management Plan
Owner	Manager Governance and Risk
Exec Owner	Chief Financial Officer
Approver	Chief Executive Officer
Date of Approval	28 October 2014
Date of Effect	28 October 2014
Next Review Date	28 October 2015
File Reference	N/A

Document Change Details *(include any policies that that this policy superceded)*

Version No.	Change Date	Changed By	Reason
0.1	11/03/2013	D Pasfield	First Draft
0.2	01/05/2013	S Srivastava	Responded to reviewer's comments
0.3	14/05/2013	S Srivastava, M Stones	Responded to reviewer's comments
0.4	27/05/13	M Stones	Removed unnecessary comments.
1.0	20/06/2013	S Srivastava, M Stones	Updated subsequent to approval by CEO.
2.0	5/9/2014	A Johnston	Updated following Privacy Audit
2.1	16/9/2014	L Tzinberg, L Rudge	Updated
2.2	10/10/14	C Herrison	Review by People and Culture
2.3	10/10/14	L Rudge	Updated

Table of Contents

Overview

Purpose

This Privacy Management Plan has two purposes. First, it meets the requirement for such a Plan under section 33 of the *Privacy and Personal Information Protection Act 1998* (NSW) (hereafter PPIP Act), by demonstrating to members of the public how Service NSW meets its privacy obligations under the PPIP Act, and the *Health Records and Information Privacy Act 2002* (NSW) (hereafter HRIP Act) and upholds and respects the privacy of our customers, employees and others about whom we hold personal information.

Second, this Plan – particularly Part C and Appendix A - acts as a reference tool for employees of Service NSW, to explain how we may best comply with the requirements of the PPIP and HRIP Acts.

Policy

Service NSW commits itself to operating in accordance with this Privacy Management Plan.

Authorisation

Approved by Glenn King, CEO
Service NSW

28 October 2014

Introduction

Introduction to Service NSW and its privacy context

Service NSW was established on 18 March 2013. Under the *Service NSW (One-stop Access to Government Services) Act 2013*, which commenced on 21 June 2013, Service NSW is given specified customer service functions (s.5) and is also allowed to disclose customer information, with an individual's consent, for the purpose of updating customer information with other agencies (s.6).

As a 'public sector agency',[1] it is regulated by the NSW privacy laws:

- the *Privacy and Personal Information Protection Act 1998* (PPIP Act), and
- the *Health Records & Information Privacy Act 2002* (HRIP Act).

The Government's Simpler Government Services Plan objectives, set out within goals 30, 31 & 32 of the State Plan NSW 2021, make a commitment to simplify customer access to government services and to design services to meet customers' needs.

The State Plan specifically identifies the establishment of Service NSW to provide:

- A single 24/7 NSW Government phone number.
- A customer friendly government web portal.
- Service Centres where multiple transactions are carried out efficiently for customers.
- Mobile applications that provide real-time information as customers need it.

It is envisioned that Service NSW will become the single Service provider of government transactional services. Transactional services in this context are defined as services generally provided to people which are non-specialist and non-complex services that can be provided in person (over the counter), over the telephone or over the internet.

Service NSW collects, holds, uses and discloses personal information for the purpose of carrying out these functions. Service NSW takes the privacy of the people of NSW and of our employees seriously, and we will protect privacy with the use of this Privacy Management Plan as a reference and guidance tool.

NSW privacy laws – *the PPIP and HRIP Acts* - centre around what are termed 'privacy principles'. The PPIP Act covers personal information other than health information, and requires agencies to comply with 12 information protection principles (IPPs). The IPPs cover the full 'life cycle' of information, from the point of collection through to the point of disposal. They include obligations with respect to data security, data quality (accuracy) and rights of access and amendment for the subject of personal information, as well as how personal

[1] The definitions of 'public sector agency' are set out at s.3 of the PPIP Act and s.4 HRIP Act. For example, the PPIP Act regulates 'Public Service Agencies' as defined under the *Government Sector Employment Act 2013*, Schedule 1 to which lists Service NSW.

information may be collected, used and disclosed. There are also specific provisions in Part 6 of the PPIP Act for managing public registers.

Health information is regulated by a slightly different set of principles. Health information includes information about a person's disability, and health / disability services provided to them. There are 15 health privacy principles (HPPs) in the HRIP Act, with which Service NSW must comply. Like the IPPs, the HPPs cover the entire information 'life cycle', but also include some additional principles with respect to anonymity, the use of unique identifiers, and the sharing of electronic health records.

There are exemptions to many of the privacy principles, the public register provisions and the definitions of 'personal information' and 'health information'. Exemptions can be found in the two Acts themselves, and in Regulations, Privacy Codes and Public Interest Directions. Where exemptions or public register provisions are particularly relevant to the Service NSW's work, they have been noted in Part C of this Privacy Management Plan.

Responsibilities of employees

All employees and contractors of Service NSW are required to comply with the PPIP and HRIP Acts.

Both Acts contain privacy principles which apply to Service NSW. If the privacy principles are breached, Service NSW may face loss of customer trust, and financial costs including compensation. Both Acts also contain criminal offence provisions applicable to employees and contractors who use or disclose personal information or health information without authority.

This Plan is intended to assist employees to understand and comply with their obligations under those Acts. If Service NSW employees feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Privacy Officer.

Employees who are suspected of conduct which would breach the privacy principles or the criminal provisions may be disciplined as for a breach of the Code of Conduct. Suspected criminal conduct may result in dismissal of employment and/or referral to NSW Police.

Warning

It is a criminal offence, punishable by up to two years' imprisonment, for any person employed or engaged by Service NSW (including former employees and contractors) to ***intentionally*** use or disclose any personal information about another person, to which the employee or contractor has or had access in the exercise of his or her official functions, except in connection with the lawful exercise of his or her official functions.

It is also a criminal offence, punishable by up to two years' imprisonment, for any person to cause any unauthorised access to or modification of restricted data held in a computer.

See s.62 of the PPIP Act, s.68 of the HRIP Act, and s.308H of the *Crimes Act 1900*.

Privacy Officer for Service NSW

Privacy Officer

Governance & Risk
Service NSW
GPO Box 7057
Sydney NSW 2001

Phone: 137788

Email: governanceandrisk@service.nsw.gov.au

Responsibilities of the Privacy Officer

The Service NSW Privacy Officer is responsible for the ongoing education of Service NSW employees (including any third party service providers, consultants or contractors) about their obligations under the PPIP and HRIP Acts, by:

- ensuring this Privacy Management Plan remains up to date;
- making a copy of this Plan available to all current and incoming employees, and contractors;
- informing employees and contractors of any changes to the Plan ensuring relevant privacy documents are consolidated and made available through the Service NSW intranet;
- conducting or arranging employee training sessions on privacy matters as required; and
- being available to answer any questions employees or contractors may have about their privacy obligations.

The Privacy Officer, in accordance with clause 6 of *the Annual Reports (Departments) Regulation 2010*, is to ensure that the Service NSW Annual Report includes:

- a statement of the action taken by Service NSW in complying with the requirements of the PPIP and HRIP Acts; and
- statistical details of any internal reviews conducted by or on behalf of Service NSW.

The Privacy Officer is to review and update this Privacy Management Plan:

- if Service NSW wishes to introduce a significant new collection of personal information; or if a privacy code or a direction of the Privacy Commissioner, or the expiry of such a code or direction, significantly modifies the application of the IPPs to the operations of the Service NSW; or at the conclusion of the 2015-16 reporting year.

The CEO of Service NSW, on the advice of the Privacy Officer, may amend this Plan as necessary at any time. A revised copy of the Plan will be made available on the website as soon as practicable. Any amendments will be drawn to the attention of all relevant personnel, and the NSW Privacy Commissioner will be advised of any such amendment as soon as practicable.

The Service NSW Privacy Officer is also responsible for answering questions from members of the public about the content or operation of the Privacy Management Plan, and handling

any privacy complaints or non-routine requests for access to or correction of personal or health information (see sections on access, correction and complaints below).

PART A: Types of personal and health information held

There are two main categories of personal information that Service NSW holds or has access to.

Customer records

These are records relating to our customers or the customers of other government agencies or organisations (our 'client agencies'). Service NSW transacts with customers through three different channels: either a Service Centre (face to face), Contact Centre (by phone) or online (website, live chat, social media or other digital facility). These transactions will fall within one of the customer service functions assigned to Service NSW in its authorising legislation, the *Service NSW (One-Stop Access to Government Services) Act 2013*.

Service NSW may hold or have access to customers' personal information in one of four ways:

1. For some client agencies, Service NSW holds no personal information in its own systems, but accesses and performs customer transactions directly in the client agency's information systems. For example:
    - Service NSW performs customer service functions on behalf of Roads and Maritime Services (RMS) by accessing and using its main customer system, DRIVES.
    - Service NSW performs customer service functions on behalf of the Registry of Births Deaths and Marriages (BDM) by accessing and using its main customer system, LifeLink.
    - Service NSW performs customer service functions on behalf of a number of other client agencies by accessing and using the Government Licensing Service, operated by the Office of Finance & Services.
2. For some client agencies, Service NSW holds and manages the primary customer records. For example:
    - Service NSW holds and manages the Seniors Card customer database on behalf of the Department of Family and Community Services. The Seniors Card customer database is held in Service NSW's SalesForce system.
3. Service NSW maintains a record of calls and email enquiries handled by its Contact Centre. This data is held in Service NSW's SalesForce system. This may include customer enquiries and/or transactions on behalf of client agencies or programs such as:
    - BDM
    - Seniors Card
    - RMS (Maritime only)
    - Energy rebates
    - Department of Planning and Environment – map viewer
    - PPP parenting courses referral

    - ASPS – referral to accredited service providers
    - Small business referrals
    - Bereavement service, and
    - random enquiries for the Government Contact Centre.
4. Service NSW also holds personal information about customers who offer feedback or make complaints about Service NSW or its client agencies. This information may be collected from sources including the Contact Centre, Service Centres, emails to the info@ line, or social media. However customer feedback data obtained from Service Centres' feedback kiosks is anonymous unless the customer adds their name to the survey.

The types of personal information held or accessed by Service NSW about customers may include:

- Identity, demographic and contact data such as name, address, telephone numbers and email address, date of birth and gender
- Data held by or on behalf of the client agency, such as details for a driver licence, birth certificate or fishing licence
- Information about transactions performed by Service NSW, such as date and time, type of enquiry or service requested, and how it was fulfilled.

Employee records

The types of personal information held by Service NSW about its employees and contractors includes:

- payroll, attendance and leave records
- performance management and evaluation records
- training records
- workers compensation records
- work health and safety records, and
- records of gender, ethnicity and disability of employees for equal employment opportunity reporting purposes.

Information on file cannot be accessed without consent of the respective employee. An employee of Service NSW may access their own file without cost under the supervision of People and Culture staff. Apart from the employee the file relates to, People and Culture Branch staff are the only other members of the agency that have authorised access to personnel files.

These records contain details including name, date of birth, home address, home phone number and emergency contact details. These records are stored in soft copy on SAP database, maintained by ServiceFirst.

ServiceFirst, a division of the Office of Finance and Services, is contracted to manage some corporate services functions for Service NSW, such as Human Resources and Finance. Therefore ServiceFirst holds and is responsible for some personal information such as recruitment, payroll and leave records. The Service Partnership Agreement between Service NSW and ServiceFirst notes that ServiceFirst will have access to information from and about Service NSW in the course of business, and that ServiceFirst is bound to comply with the PPIP Act. The Agreement states:

"Such information will be used strictly for purposes relevant to delivering services and will not be released to third parties without the express written consent of Service NSW."

Service NSW may also hold other miscellaneous personal information such as correspondence with members of the public (other than in relation to the performance of customer service functions).

PART B: Inventory of significant information systems

With respect to customers' personal information, Service NSW's main information system is SalesForce. All other information systems which hold customers' personal information are managed by our client agencies. See Part A of this Privacy Management Plan for more details.

With respect to employees' and contractors' personal information, Service NSW, or other agencies or contractors acting on its behalf, will keep personal information in a variety of administrative information systems, including SAP - Corporate HR and Finance systems, records management systems and other standard Office-based products.

PART C: How the privacy principles apply

Important note about using this Part

This Part of the Privacy Management Plan uses plain language, not the exact wording of the law to describe the privacy principles and how Service NSW employees and contractors will comply with them. This is to make understanding our obligations a little easier. This document does not cover the full complexity of the privacy laws applying to Service NSW. It has been simplified, and does not cover all exemptions or situations. If in doubt, you should always check the exact wording in the legislation, and seek guidance from the Service NSW Privacy Officer, or the NSW Privacy Commissioner. This document is an educational tool, not legal advice.

Introduction

Our privacy obligations have been condensed into one set of 12 plain language principles to be followed by Service NSW as follows (references in brackets are to the principles in the PPIP and HRIP Acts):

- limiting our collection of personal information (IPP 1 and HPP 1)
- anonymity and identifiers (HPPs 12 and 13)
- how we collect personal information – the source (IPP 2 and HPP 3)

- how we collect personal information – the method and content IPP 4 and HPP 2)
- notification when collecting personal information (IPP 3 and HPP 4)
- security safeguards IPP 5 and HPP 5)
- transparency (IPP 6 and HPP 6)
- access (IPP 7 and HPP 7)
- correction (IPP8 and HPP 8)
- accuracy (IPP 9 and HPP 9)
- use (IPP 10 and HPP 10)
- disclosure (IPPs 11 and 12, and HPPs 11, 14 and 15)

This Part of the Privacy Management Plan outlines key definitions, and for each of the plain language privacy principles:

- a summary description
- when there are different rules for 'sensitive or 'health' information
- some key points about how the privacy principles work in practice in the context of Service NSW's functions, and
- any relevant exemption.

Which information?

This part of the Privacy Management Plan relates mainly to the way in which Service NSW handles customer records. It does not comprehensively address employee records which are handled in accordance with generic policies for the NSW public service. For example, employee records may be administered in accordance with NSW Government Policies available through the Employment Portal at www.psc.nsw.gov.au.

Relationship with client agencies

Service NSW is somewhat unusual in that the majority of the customer personal information it handles will be for the purpose of fulfilling a transaction on behalf of another government agency or organisation (our 'client agencies'), and compliance with the privacy principles will primarily be the responsibility of that agency. Client agencies will specify through Service Partnership Agreements with Service NSW their requirements in terms of the personal information that needs to be collected, and how it is to be processed on behalf of that agency. Service NSW will be responsible for complying with those requirements, including ensuring data security and data quality. Service NSW is primarily responsible for any customer data which it maintains for internal administrative purposes, as well as customer data collected into or via the SalesForce system.

Definitions

Collection of personal information	The way Service NSW acquires the information. Collection can be by any means. Examples include: a written form, a verbal conversation, an online form, a voice recording or taking a picture or image.
Disclosure	When we provide personal information to an individual or body outside Service NSW, including to a client agency.

GIPA Act	The *Government Information (Public Access) Act 2009 (NSW).*
Health information	A special types of 'personal information' (see below). Some of our privacy obligations are different for 'health information'. It 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 services to him or her • other personal information collected to provide a health service, or in providing a health service • information about the intended or actual donation of organs or body parts • genetic information that is or could be predictive of the health of a person or their relatives or descendants, or • healthcare identifiers.
Holding personal information	Most of our privacy obligations apply to personal information that we 'hold'. Service NSW will be considered to be 'holding' personal information if it is in our possession or control. 'Control' can include the ability to view or edit information by virtue of our access to client agencies' information systems. It is possible for more than one organisation to 'hold' personal information at the same time. For example, customer data entered into DRIVES by a Service NSW employee member will be possessed by RMS, but also within the control of Service NSW.
HRIP Act	The *Health Records & Information Privacy Act 2002 (NSW)*. The HRIP Act contains 15 Health Privacy Principles (HPPs).
Personal information	Any information or an opinion about an individual whose identity is apparent or can reasonably be ascertained. The information does not have to be considered 'private'. Personal information can include information that is recorded (e.g. on paper or contained in a database), but also information that is not recorded (e.g. verbal conversations or observations).
PPIP Act	The *Privacy and Personal Information Protection Act 1998 (NSW)*. The PPIP Act contains 12 Information Protection Principles (IPPs).
Privacy obligations	The IPPs and the HPPs, as interpreted by Service NSW in the context of its functions and subject to any exemptions to those principles that apply.
Sensitive information	A special types of 'personal information' (see above). Some of our privacy obligations are different for 'sensitive information'. It means personal information that is also about a person's race, ethnicity, religion, sexuality, political or philosophical beliefs or membership of a trade union.
Use	Refers to the use of personal information by or on behalf of Service NSW for some purpose, as distinct from disclosure to third parties (see above).

1. Limiting our collection of personal information

1.1. The principle in brief

We will only collect personal 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.

1.2. Key points

We won't ask for personal information unless we need it for one of our customer service functions, for the purpose of updating contact details with an individual's consent, or for internal administrative purposes. We will especially avoid collecting sensitive information if we don't need it.

By limiting our collection of personal information to only what we need, it is much easier to comply with our other obligations. Often our client agencies are responsible for defining what customer information is needed to fulfil a transaction. In other circumstances, such as the Contact Centre, we will need to ensure that only the minimum amount of information is collected or recorded, in order to fulfil our customer service functions.

2. Anonymity and Identifiers

2.1. The principle in brief

We will allow people to receive services from us anonymously, where lawful and practicable. We will only assign identifiers (such as customer numbers) to customers where required to do so by our client agency.

Example: People making informal enquiries or requesting general information, should not be required to identify themselves.

3. How we collect personal information – the source

3.1. The principle in brief

We collect personal information directly from the person unless they have authorised otherwise or, in the case of health information, it would be unreasonable or impractical to obtain the information directly from the person. We will acquire much information from other agencies on whose behalf Service NSW is performing customer service functions, but this will generally be at the request of the individual concerned.

3.2. Key points

Some of Service NSW's customer service functions will relate to transactions that require exchange or verification of personal information with third parties, and in such cases collection may not be with the individual's express authorisation, although it will often be a condition of the transaction they are seeking to perform. Compliance with this principle

will largely be the responsibility of client agencies, effected through the procedures included under Service Partnership Agreements.

Collection of personal information by Service NSW for its own internal administration purposes should not require collection via third parties. By collecting information direct from the source, it will be easier for us to comply with other obligations too, like ensuring the accuracy of the information, and getting permission for any secondary use or disclosure of the information.

3.3. Other relevant points

Where the person is under 16, we may collect their personal information from their parent or guardian. Where a person aged 16 or over lacks some capacity (e.g. because of mental illness, intellectual disability, dementia, brain injury, illness, accident or disease), we can ask their authorised representative for the information instead. However, we must also still try to communicate with them directly. The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities*[2] explains how to collect personal information from or about a person who has limited or no capacity.

The NSW Privacy Commissioners *Handbook to Health Privacy*[3] provides some other examples of when it might be "unreasonable or impractical" to collect health information directly from the person.

4. How we collect personal information – the method and content

4.1. The principle in brief

- We will not collect personal information by unlawful means.
- We will not collect personal information that is intrusive or excessive.
- We will ensure that the personal information we collect is relevant, accurate, up-to-date, complete, and not misleading.

4.2. Key points

Service NSW will always ensure that collection is lawful. The types of personal information collected in the Service Centre and Digital channels are defined for us by our client agencies. In our Contact Centre, employees who record information from callers must be mindful of this principle, and only record in SalesForce the minimum information necessary in order to provide the service requested.

Inbound calls to the Service NSW Contact Centre will normally be recorded. Callers do not have a choice whether their call will be recorded but notice will be given (see 5 below). Recording with prior notice complies with the participant monitoring provisions of the *Telecommunications (Interception and Access) Act 1979* (Cth) as well as NSW privacy and surveillance laws.

Ensuring that personal information is of high quality will of course be a constant challenge, particularly given the range of transactions that Service NSW will perform. However, it is

[2] Available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies
[3] Available from http://www.ipc.nsw.gov.au/hrip-act

reasonable to assume that individuals using Service NSW will generally give us information that is 'fit for purpose', and regular customer contact provides an opportunity to check accuracy of data with individuals, where that is appropriate. Where appropriate, Service NSW uses automated techniques to ensure that such details as addresses and telephone numbers are in the correct format.

5. Notification when collecting personal information

5.1. The principle in brief

When collecting personal information, we will take reasonable steps to tell the person:

- who will hold and/or have access to their personal information
- what it will be used for
- what other organisations (if any) routinely receive this type of personal information from us
- whether the collection is required by law
- what the consequences will be for the person if they do not provide the information to us, and
- how the person can access their personal information held by us.

5.2. Key points

For many transactions, Service NSW will provide customers with privacy notices supplied by client agencies to meet their notification obligations e.g. on client agency paper or online forms, or in relevant telephone scripts. In addition, Service NSW will ensure that customers are notified when Service NSW is collecting personal information for its own internal management purposes. This will be delivered through a variety of channels, including pre-recorded voice messages and printed and online notices. Service NSW adopts a layered approach to privacy notices, as endorsed by the Privacy Commissioner, to avoid overloading customers with too much information which many may not want. A concise basic notice will include information about how to obtain more detail if wanted.

5.3. Other relevant points

A *Guide to drafting privacy notices* is attached in Appendix A to this document. This can be used as the starting point for drafting notices to be delivered through different channels. Any new projects or changes which might collect new personal information or allow for new purposes should be reviewed by the Service NSW Privacy Officer to ensure an adequate privacy notice is included.

For Non-English speaking background customers, the NSW Privacy Commissioner's *Community Language Privacy Notice*[4] should be used. The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities*[5] explains how to notify a person who has limited capacity to understand.

[4] Available from http://www.ipc.nsw.gov.au/community-language-notices
[5] Available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies

In the case of inbound calls to the Contact Centre, a recorded message will give notice that the call may be recorded or monitored. Contact Centre employees making outbound calls must provide the notice themselves.

6. Security safeguards

6.1. The principle in brief

We will take reasonable security measures to protect personal and health information from loss, unauthorised access, modification, use or disclosure. We will ensure personal information is stored securely, not kept longer than necessary, and disposed of appropriately.

6.2. Key points

Security measures include technical, physical and administrative actions.

Service NSW information systems are designed to ensure that only authorised users can access them, and then only give access to information required for the user's particular role and functions. Transaction logs or audit trails will act as a deterrent against any misuse, and also allow security breaches or data quality issues to be investigated.

Security considerations are taken into account in arrangements for data transmission (including encryption where appropriate), backup and storage.

Service NSW applies disposal schedules in accordance with the *State Records Act 1998* in relation to retention periods and disposal.

7. Transparency

7.1. The principle in brief

We will enable anyone to know:

- whether we are likely to hold their personal information
- the purposes for which we use personal information, and
- how they can access their own personal information.

7.2. Key points

We have a broad obligation to the community to be open about how we handle personal information. This is different to collection notification, which is much more specific, and given at the time of collecting new personal information.

This Privacy Management Plan will be accessible through our website. It sets out the major categories of personal information that we hold and explains our privacy obligations. Persons wanting more information or explanation can request it through the Service NSW Privacy Officer.

8. Access

8.1. The principle in brief

We will allow people to access their personal information without unreasonable delay or expense. We will only refuse access where authorised by law. If requested, we will provide written reasons for any refusal.

8.2. Key points

Where individuals seek access to information we hold about them in relation to a transaction with a client agency, we will normally refer them to that agency to process their request, unless the relevant Service Partnership Agreement with that client agency has provided for us to do this on their behalf.

Many customer service requests processed by Service NSW on behalf of client agencies could be construed incidentally as requests for personal information; e.g. 'Is my licence current? What are the conditions of my permit? Such requests will be handled in accordance with specifications set out in the Service Partnership Agreement with the relevant agency, rather than treated as access requests under either the PPIP, HRIP or GIPA Acts.

People should generally be able to see what information Service NSW holds about them independently from transactions for client agencies, with a minimum of fuss. Our policy is that as far as possible, customers, employees and other individuals can make a request to see their own personal information at no cost. Requests can be made by phone, email or in person.

We cannot charge people to lodge their request for access. But we can charge reasonable fees for copying or inspection, if we tell people what the fees are up-front. Fees will be no more than we would charge for access under the GIPA Act, which allows up to $30 per hour for the work it takes to identify the information sought and consider whether it may be released. If there is personal information about other individuals or confidential information about third parties in any records identified by our searches, then the Privacy Officer will process the request for access, rather than the area that holds the record. This will ensure that the privacy and confidentiality of other people and third parties can also be properly considered.

8.3. Exemptions

Before you rely on an exemption, check with the Service NSW Privacy Officer.

In some circumstances, another law may prevent us from giving the person access to the information requested.

8.4. Other relevant points

The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities*[6] explains how to provide access to personal information held about a person

[6] Available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies

who has limited or no capacity. Formal access applications under the GIPA Act will be handled by the Service NSW Privacy Officer.

If there is any doubt about whether a request for access to personal information is from the individual to whom the information relates or their authorised representative, the request should be referred to the Service NSW Privacy Officer.

9. Correction

9.1. The principle in brief

We will allow people to update or amend their personal information, to ensure it is accurate, relevant, up-to-date, complete or not misleading.

9.2. Key points

For Service NSW, correction of customer information is more than just an obligation under privacy law – it is core business, as part of our customer service functions. We will actively encourage and remind customers to keep any information we hold about them accurate, up to date and complete, to the extent that they wish to do so.

When an individual requests a change to their contact details, either in relation to a specific transaction or more generally, Service NSW may offer them choices in respect of updating information held by other government agencies.

If we disagree with an individual about whether the information needs changing (for example if we have determined that the information held is an accurate record), we can decline to do so, but must instead allow the person to add a statement or notation to our records. We cannot charge individuals for requesting for amendment, or for processing such a request or for making an amendment.

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

9.3. Exemptions

Before you rely on an exemption, check with the Service NSW Privacy Officer. We can decline to make an amendment if another law authorises or requires us to not to do so, although the correction right in privacy laws overrides ‘non-alteration’ provisions of the *State Records Act 1998*.

9.4. Other relevant points

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

10. Accuracy

10.1. The principle in brief

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

10.2. Key points

For most of Service NSW's functions, checking information before use or disclosure will be 'built in' to normal operating procedures, e.g. asking customers to verify their personal information while processing a transaction.

Verification may require extra steps where we use or disclose personal information for secondary purposes, including under one of the exemptions (see below). However, we only need to take reasonable steps to check the information – although more steps will be needed if the use or disclosure may disadvantage the person, e.g. prior to disclosure to a law enforcement agency.

What might be considered "reasonable steps" will depend upon the circumstances, but some points to consider 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.

Example: If Service NSW received information from a third party that your details had changed we would contact you to verify the information with you prior to amending your information.

11. Use

11.1. The principle in brief

We may use personal information:

- for the primary purpose for which it was collected, or
- for a directly related secondary purpose, or
- if Service NSW reasonably believes that the use is necessary to prevent or lessen a serious and imminent threat to life or health, or
- for another purpose if the person has consented.

11.2. Key points

The primary purpose for which we use customers' personal information will be one or more of our customer service functions. The primary purpose should have been set out in a privacy notice for that particular service.

A directly related secondary purpose will be used for our internal administrative records. (For example, if the primary purpose of collecting a complainant's information was to investigate their customer complaint, then independent auditing of our complaint-handling practices would be an acceptable use for a directly related secondary purpose.)

With consent, we may also use a customer's personal information for updating their contact information with other agencies.

To use personal information for any other purpose, check with the Service NSW Privacy Officer first.

The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities*[7] explains how to seek consent for a secondary use of personal information from a person who has limited or no capacity. The NSW Privacy Commissioner's *Statutory Guidelines on Research*[8] explain how health information can be used for research purposes. It also provides a good rule of thumb for the use of other types of personal information for research purposes.

11.3. Exemptions

Before you rely on an exemption, check with the Service NSW Privacy Officer.

Service NSW may use personal information without consent in specified circumstances:

- if another law authorises or requires us to use the information
- for some law enforcement and investigative purposes, or
- for some research purposes, subject to approval by a Human Research Ethics Committee.

Use of information in any of these circumstances is also likely to involve disclosure, in which case the somewhat different exemptions apply – see below.

12. Disclosure

12.1. The principle in brief

We may disclose personal information if:

- the person has consented, or
- the information is not 'health information' or 'sensitive information', and the individual has been made aware that the information is likely to be disclosed to the recipient, or
- the information is not 'health information' or 'sensitive information', and the disclosure is directly related to the purpose for which the information was collected, and Service NSW has no reason to believe that the individual concerned would object to the disclosure, or

[7] Available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies
[8] Available from http://www.ipc.nsw.gov.au/hrip-act

- the information is ‘health information’, and the disclosure is for the purpose for which the information was collected, or for a directly related secondary purpose within the person’s reasonable expectations.

12.2. Stricter rules apply to specific information

Disclosing ‘sensitive information’ is generally only allowed with the person’s consent.

We can only transfer ‘health information’ outside of NSW (including to the Commonwealth Government), if one of the following applies:

- the person concerned has consented
- it is necessary for a contract with (or in the interests of) the person concerned
- it will benefit the person concerned, we cannot 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, or
- we have bound the recipient by contract to privacy obligations equivalent to the HPPs.

12.3. Key points

Most disclosures by Service NSW in the course of its customer service functions or updating customer information with other agencies will be not only ‘related’ to the primary purpose and within the individual’s reasonable expectations but also explained in a privacy notice – meeting two of the conditions in the disclosure principles.

Disclosure of personal information about a customer to the client agency on whose behalf Service NSW is operating is authorised by s.14 of the *Service NSW (One-stop Access to Government Services) Act 2013*.

Disclosures for any other purpose need to be tested against the exemptions, outlined below. Before disclosing personal information for any other purpose, or if in doubt, check with the Service NSW Privacy Officer. Requests for personal information from outside bodies, including from government agencies which are not clients of Service NSW, and from client agencies for information unrelated to the functions Service NSW is performing for them, should be referred to the Service NSW Privacy Officer to assess whether an exemption applies.

12.4. Exemptions

Before you rely on an exemption, check with the Service NSW Privacy Officer.

Service NSW may also disclose personal information without consent in specified circumstances:

- if we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health
- if it is ‘health information’, and we reasonably believe that the disclosure is necessary to deal with a serious threat to public health or safety
- if another law authorises or requires us to disclose the information

- if a subpoena, warrant or 'notice to produce' requires us by law to disclose the information
- for some law enforcement and investigative purposes
- some research purposes, subject to approval by a Human Research Ethics Committee, or
- exchanges of information which are reasonably necessary to allow agencies to deal with or respond to correspondence from Ministers or Members of Parliament, or to refer inquiries between agencies.

12.5. Other relevant points

The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities*[9] explains how to seek consent for a disclosure of personal information from a person who has limited or no capacity. The NSW Privacy Commissioner's *Statutory Guidelines on Research*[10] explain how health information can be disclosed for research purposes. It also provides a good rule of thumb for the disclosure of other types of personal information for research purposes.

PART D: Privacy and other legislation relating to personal and health information

Privacy legislation

- Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)
- Health Records & Information Privacy Act 2002 (NSW) (HRIP Act)
- Privacy and Personal Information Protection Regulation 2014
- Health Records and Information Privacy Regulation 2012
- Codes of Practice, Directions and Statutory Guidelines made under the PPIP and HRIP Acts

Other relevant legislation

- Crimes Act 1900
- Government Information (Public Access) Act 2009
- State Records Act 1998
- Workplace Surveillance Act 2005

PART E: Policies affecting

[9] Available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies
[10] Available from http://www.ipc.nsw.gov.au/hrip-act

processing of personal and health information

- Service NSW *Code of Conduct*. Section “Using and protecting confidential information” and Section “Responsibilities, accountabilities and expectations” relate to confidentiality, the security of information, and compliance with privacy obligations.
- Service NSW *Internet and Email Usage Policy*
- Service NSW *Media and Social Media Policy*

PART F: Privacy complaints

Any person may make a privacy complaint:

1. Directly to the NSW Privacy Commissioner, or
2. by applying to Service NSW for an ‘internal review’ of the conduct they believe breaches an IPP and/or an HPP.

Complaints direct to the Privacy Commissioner can result in conciliated outcomes, whereas internal review can lead to a binding determination by the NSW Civil & Administrative Tribunal (NCAT), including an award of compensation of up to $40,000.

Internal review is the process by which Service NSW manages formal, written privacy complaints about how we have dealt with personal 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’.

Under the privacy laws, an application for internal review must:

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

Service NSW encourages the use of its *Internal Review Application Form*, found at Appendix B to this Privacy Management Plan.

An application for internal review can be made on behalf of someone else. Where the applicant is not literate in either English or their first language and where there is no other organisation making the application on their behalf, employees should help the person to write their application. Employees should use a professional interpreter, if necessary.

Applications for internal review, or any written complaint about privacy, received at any of Service NSW’s premises should be forwarded immediately to the Service NSW Privacy Officer.

If the complaint is about an alleged breach of the IPPs and/or HPPs, the internal review will be conducted by the Service NSW Privacy Officer, or by another person who:

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

Extensions of time for lodgement

While the PPIP Act allows applicants six months to apply for an internal review from the time the applicant first becomes aware of the conduct, and their right to seek internal review. Service NSW 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 an earlier time.

However late applications that, because of their age, cannot be investigated in a meaningful way will be declined. In these cases, witnesses may no longer be available, documents may have been destroyed and memories may have faded. Final decisions on the acceptance of late applications will only be made by the Privacy Officer or under his/her delegation. Where the decision is made not to accept an application because it is too old, the reason will be explained in a letter to the applicant.

The Internal Review process

When Service NSW receives an internal review application the Service NSW Privacy Officer will:

- determine whether the internal review should be handled by Service NSW alone, the client agency alone, or jointly. The applicant's consent will be sought before a copy is forwarded to the client agency;
- send an acknowledgment letter to the applicant and advise that if the internal review is not completed within 60 days they have a right to seek a review by NCAT; and
- send a letter to the NSW Privacy Commissioner with details of the application.

A photocopy of the written complaint will also be provided to the Privacy Commissioner.

Internal reviews follow the process set out in the NSW Privacy Commissioner's *Internal Review Checklist*.[11] The Privacy Commissioner may make submissions to Service NSW as part of the internal review process.

When the internal review is completed, the Service NSW Privacy Officer will notify the applicant in writing of:

- the findings of the review
- the reasons for the finding, described in terms of the IPPs and/or HPPs

[11] Available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies

- any 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 NCAT.

We will also send a copy of that letter to the NSW Privacy Commissioner.

Statistical information about the number of internal reviews conducted must be maintained for the Service NSW Annual Report.

External Review by the NSW Civil & Administrative Tribunal (NCAT)

People may apply to NCAT for an external review of the conduct which was the subject of their earlier internal review application. NCAT may make orders requiring Service NSW to:

- refrain from conduct or action which breaches an IPP, HPP or Code
- perform in compliance with an IPP, HPP or Code
- correct or provide access to information
- provide an apology, or
- take steps to remedy loss or damage.

NCAT may also make an order requiring the Agency to pay damages of up to $40,000 if the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

PART G: Strategies for implementing and reviewing this Plan

Service NSW's first Privacy Management Plan was drafted in early 2013.

This edition was drafted in mid-2014.

Service NSW commissioned a privacy audit of its operations in 2014. The privacy audit identified a number of areas of improvement for Service NSW, in terms of ensuring compliance with the IPPs and HPPs. Key recommendations covered:

- better employee awareness and training on privacy issues and practices,
- changes to procedures, forms, notices and client agency agreements,
- improved records management, and
- incorporating the full range of privacy principles into new and existing information technology systems.

Service NSW has made it a priority implement these recommendations during 2014-15. A privacy implementation communications plan has been developed to create visibility of Service NSW privacy resources.

The Service NSW Privacy Officer is responsible for the governance of the Privacy Plan, and will oversee the regular review and update of the plan every two years or earlier if required.

If you have any feedback on this document please contact the Service NSW Privacy Officer: by mail at GPO Box 7057 Sydney NSW 2001, by phone to 137788, or by email to governanceandrisk@service.nsw.gov.au

APPENDIX A: Guide to drafting privacy notices

Service NSW has adopted a policy position that it will be responsible for delivering a privacy notice for every customer transaction.

The following principles are to guide the process for drafting privacy notices for customer service transactions:

- the Service NSW Privacy Officer must approve the wording and location of all privacy notices;
- the client agency must approve the wording of the privacy notice;
- if the transaction can occur across more than one service channel, the privacy notice should be worded as closely as possible across each channel.

  However there will need to be some differences for the Contact Centre channel. For example, in the Digital or Service Centre channels, a mandatory field is easily denoted by an asterix on the online or paper form. While the design of a SalesForce data entry field may also allow for this, the script for Contact Centre operators may need additional verbal explanation for the customer;

- wording should be concise and in plain language;
- the notice should clarify what Service NSW will do with the information, as well as what the client agency will do with the information;
- the notice should be given / visible before any data collection begins;
- in the Service Centre channel, notice can be provided on the paper forms developed and supplied by the client agency;
- in the Digital channel, the notice should be given on the landing page for that transaction, even if it also appears later on in the process; and
- in the Digital channel, if the data is actually being collected and stored by Service NSW (such as for the Seniors Card database), the notice should also appear on the first data collection page.

At the end of the privacy notice developed for each specific type of collection, further information should be added, such as:

> For further information about privacy, see www.service.nsw.gov.au/privacy, or contact the Service NSW Privacy Officer: by mail at GPO Box 7057 Sydney NSW 2001, by phone to 137788, or by email to governanceandrisk@service.nsw.gov.au

APPENDIX B: Privacy Complaint (Internal Review Application) Form

(please see next page for copy of form)

Privacy Complaint (Internal Review Application) Form

You should use this form if you wish make a complaint about the way Service NSW has handled personal information, either on behalf of a client agency, or in relation to its own purposes.

Note: Service NSW is a gateway for transactions with a wide range of other [NSW] government agencies. If your complaint relates to a transaction with another agency, and Service NSW considers that it is more appropriately dealt with by that agency, we will contact you and request your consent for us to transfer the complaint to that agency. Other agencies will have their own complaint processes and may contact you about their requirements.

Your details			
Name of the Agency you are complaining about			
Your full name			
Your postal address			
If you are complaining on behalf of someone else, write their full name here			
What is your relationship to this other person? (e.g. parent or lawyer):		Is the other person capable of making the complaint him or herself?	❑ Yes ❑ No ❑ I'm not sure

Your complaint	
What is the specific conduct you are complaining about? :	***Note: 'Conduct' can include an action, a decision, or even inaction by Service NSW. For example the 'conduct' in your case might be a decision to refuse you access to your personal information, or the action of disclosing your personal information to another person, or the inaction of a failure to protect your personal information from being inappropriately accessed by someone else.)***
Please tick which of the following describes your complaint: (You can tick more than one)	❑ Collection of my personal/health information ❑ Security or storage of my personal/health information ❑ Refusal to let me access or find out about my own personal/health information ❑ Accuracy of my personal/health information ❑ Use of my personal/health information ❑ Disclosure of my personal/health information ❑ Other ❑ I'm not sure

When did the conduct occur? (Please be as specific as you can):	***Note: You need to lodge this application within 6 months of the date you have written at Q.8. If more than 6 months has passed, you need to ask the Service NSW Privacy Officer for special permission to lodge a late application. If you need to, write here to explain why you have taken more than 6 months to make your complaint.***
When did you first become aware of this conduct?	
What effect did the conduct have on you?	
What effect might the conduct have on you in the future?	
What would you like to see Service NSW do about the conduct?	***For example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.***

Acknowledgement

- I understand that this form will be used by Service NSW to process my request for an Internal Review, and that the Internal Review may be conducted jointly with the client agency.
- I understand that details of my application will be referred to the NSW Privacy Commissioner as required by law, and that the Privacy Commissioner will be kept advised of the progress of the review.

I would prefer the Privacy Commissioner to have:

❑ A copy of this application form, or

❑ Just the information provided in the "Your complaint" section of this document.

Your signature	
Date:	

Now send this form to:

Privacy Officer
Service NSW
GPO Box 7057
Sydney NSW 2001
Phone: 137788
Email: governanceandrisk@service.nsw.gov.au

Keep a copy for your own records too.