Privacy Management Plan

October 2019

Policy Statement

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 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.

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

Approved by			
Name:	Damon Rees		
Title:	Chief Executive Officer	**Date:**	October 2019

Privacy Management Plan

October 2019

Table of Contents

Introduction

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', 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 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.

Our stakeholders

We may collect personal or health information from, or disclose personal or health information to, our stakeholders to do our work. These stakeholders include:

- members of the public
- workers
- persons conducting a business or undertaking
- insurers
- other regulators
- other law enforcement agencies
- other, local, state and federal government agencies and authorities
- private sector companies
- academics and researchers
- medical and allied health professionals
- non-government organisations
- solicitors and other legal representatives
- courts and tribunals
- Ministers and Parliament

Definitions

Agency	A 'public sector agency', as defined in section 3 of the PPIP Act
Business Unit	This is a reference to a work unit performing a discrete business function. Multiple business units make up divisions.
DCS or Department of Customer Service	Refers to the Department of Customer Service cluster

Division	this is a reference to a broad business area within the Department of Customer Service, often comprised of multiple business units. There are five divisions in DCS: Service NSW, Customer, Delivery and Transformation, Better Regulation, Digital and ICT, and Corporate Services
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.
Disclose	Service NSW's discloses personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control.
GIPA Act	The *Government Information (Public Access) Act 2009 (NSW).*
Health Information	as defined in section 6 of the HRIP Act, health information is a specific type of 'personal information'. It includes but is not limited to: • information or an opinion about a person's physical or mental health, or a disability (at any time), such as a psychological report, blood test or x-ray • personal information a person provides to a health service provider • information or an opinion about a health service already provided to a person eg. attendance at a medical appointment • information or an opinion about a health service that is going to be provided to a person • a health service a person has requested • some genetic information.
Health Privacy Principles or HPPs	Refers to the 15 Health Privacy Principles set out in Schedule 1 of the HRIP Act
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).
Information Protection Principles or IPPs	Refers to the 12 Information Protection Principles set out in Part 2, Division 1 of the PPIP Act
Personal information	as defined in section 4 of the PPIP Act, personal information is information or an opinion that identifies a person (or that would allow a person's identity to be discovered). Personal information can include: • person's name, address, financial information and other details • photographs, images, video or audio footage • fingerprints, blood or DNA samples. Some types of personal information are exempt from the definition of personal information e.g. information about a person that has been dead for more than 30 years, information about someone that is contained in a publicly available publication or information or opinion about a person's suitability for employment as a public sector official.
PIPP 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	Means information referred to in section 19(1) of the PPIP Act. A special type 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.

Service Partnership Agreement	The agreement Service NSW enters into with client agencies, which stipulates the terms, conditions, requirements, specifications and responsibilities regarding the transactions Service NSW completes on the agency's behalf
Use	As defined where Service NSW handles or undertakes an activity with information, within Service NSW's effective control
PMP	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.

It is an offence to:

- intentionally disclose or use personal or health information accessed in doing our jobs for an unauthorised purpose
- offer to supply personal or health information for an unauthorised purpose
- attempt by threat, intimidation, etc, to dissuade a person from making or pursuing a request for health information, a complaint to the NSW Privacy Commissioner about health information, or an internal review under the HRIP Act, or
- hinder the Privacy Commissioner or member of staff from doing their job.

WARNING

It is a criminal offence, punishable by up to two years' imprisonment, an $11,000 fine, or both, for any person employed or engaged by Service NSW (including former employees and contractors) to intentionally use, disclose or offer to supply any personal information or health 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 the 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 actions 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 Service NSW; or at the conclusion of the 2019-20 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

Personal Information

When we use the term 'personal information' we adopt the definition in the PPIP Act (see Definitions in the Introduction section).

Health Information

When we use the term 'health information' we adopted the definition in the HRIP Act (see Definitions in the Introduction section).

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.

Day to day operations of most staff, such as leave requests and payroll, are administered by an outsourced company called GovConnect. An Outsourcing Agreement was developed under the outsourcing program when GovConnect was engaged. It includes contractual arrangements providing that contractors must comply with the *Privacy Act 1988* (Cth), the PPIP and HRIP Acts, as well as any other privacy codes and policies in force, to ensure employees' personal information is protected.

Therefore, GovConnect holds and is responsible for some personal information such as recruitment, payroll and leave records. The Service Partnership Agreement between Service NSW and GovConnect notes that GovConnect will have access to information from and about Service NSW in the course of business, and that GovConnect 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

There are 12 Information Protection Principles (IPPs) set out in Part 2, Division 1 of the PPIP Act and 15 Health Privacy Principles (HPPs) set out in Schedule 1 of the HRIP Act. The Information and Privacy Commission has issued fact sheets setting out the principles in summary. These fact sheets are attached at Appendix 1.

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.

The Privacy Principles

1. Limiting our collection of personal information (IPP1 [PPIP s8] and HPP 1)

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. How we apply this principle

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 Unique Identifiers (HPP 12, 13 and 15)

2.1. The principle in brief – general anonymity where possible

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.

In relation to health information, we may only assign identifiers (e.g. a number) to an individual's health information if it is reasonably necessary. We must not include health information in a health records linkage system without your consent.

2.2. How we apply this principle

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

Service NSW takes care to ensure it does not inadvertently collect health information of customers. When this sort of information is collected, it is not given any separate identifier and it not included in any health records linkage system.

People & Culture may collect health information in order to manage cases of injured staff and to investigate workplace incidents. Where health information has been gathered to case manage an injured staff member, it is not given a separate identifier but kept against the relevant employee's injury management record. Where the information has been

gathered as part of an investigation of a workplace incident, the information is held against the investigation file, and not given any separate identifier. People and Culture have no linkages to any health records systems.

3. How we collect personal information – the source (IPP 2 [PPIP s9] and HPP 3)

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. How we apply this principle

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* 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* 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 (IPP 4 [PPIP s11] and HPP 2)

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. How we apply this principle

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 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.

A substantial amount of personal and health information is collected from our staff for the purpose of personnel management. Such information is stored securely by the People and Culture unit and GovConnect, which have a centralised human resources management role. Personal and health information may also be collected directly from the staff member within a division, when it is lawfully authorised and necessary for staff management. For example, minimal health information may be collected by your direct manager for the purpose of making necessary adjustment to allow you to work, or for creation of a return-to-work plan.

5. Notification when collecting personal information (IPP 3 [PPIP s 10] and HPP 4)

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. How we apply this principle

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. Relevant points

A *Guide to Drafting Privacy Notices* is attached in Appendix 4 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* should be used. The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities* explains how to notify a person who has limited capacity to understand.

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 – storage of personal and health information (IPP 5 [PPIP s12] and HPP 5)

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. How we apply this principle

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.

All employees, including contractors, are required to comply with the Service NSW *Code of Conduct* and Service NSW *Information Security Policy*. The *Information Security Policy* sets out the actions Service NSW takes to secure information, including maintaining an Information Security Management System compliant with ISO27001:2013. For more information about how we ensure information security, refer to the *Information Security Policy*.

Security considerations are taken into account in arrangements for data transmission (including encryption where appropriate), backup and storage. Generally, once data is entered into the secure system, any paper documents are shredded or sent for secure destruction to ensure that they cannot be accessed inappropriately.

Service NSW applies disposal schedules in accordance with the *State Records Act 1998.* In divisions that deal with substantial amounts of private or sensitive information, such as human resource units or investigation teams, access to the floor or the room where personal information is stored may be restricted to authorised personnel.

7. Transparency (IPP 6 [PPIP s13] and HPP 6)

7.1. The principle in brief

Once a person has confirmed their identity, will we take reasonable steps to allow a person to find out:

- whether we are likely to hold their personal information
- the nature of the information we hold
- the purposes for which we use personal information, and
- how a person can access their own personal information

7.2. How we apply this principle

We have a broad obligation to the community to be open about how we handle personal and health information. This is different to a 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 to information we hold (IPP 7 [PPIP s14] and HPP 7)

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. How we apply this principle

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* explains how to provide access to personal information held about a person who has limited or no capacity. Formal access applications under the GIPA Act will be handled by the Service NSW Privacy Officer or equivalent authorised personnel.

If there is any doubt about whether a request 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 or equivalent authorised personnel.

9. Correction of information we hold (IPP 8 [PPIP s15] and HPP 8)

9.1. The principle in brief

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

9.2. How we apply this principle

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 of information (IPP 9 [PPIP s16] and HPP 9)

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. How we apply this principle

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 – how we use personal and health information (IPP 10 [PPIP s 17] and HPP 10)

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. How we apply this principle

As a general principle, we use the personal and health information we've collected only for

the purpose for which it was collected. 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* 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* 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.

How we use the personal and health information of employees

If you are a Service NSW employee, your personal and health information will be used for personnel management, such as salary payments, wellbeing in the workplace, and performance management. You have unlimited access to any of your personal information that is held by the agency, for example, through SAP and MyCareer. This includes your payslips, leave balances, comments from your supervisor, timesheets and other types of personal information. You are also entitled to access your personnel file, ATLAS or any other related human resources or employee safety and wellbeing files that contain your personal or health information.

Some information is maintained at a local divisional level, or is accessed by divisions for management purposes. This includes storing and using employees' personal and health information on internal databases for management purposes (including staff resource planning), case review and training. You can request access to and amend your personal or health information at any time. This information will be updated without excessive delay.

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 – how we disclose personal and health information (IPP 11 [PPIP s18] and HPP 11)

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
- 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 (IPP 12 [PPIP s19] and HPP 14)

Disclosing sensitive information (e.g. your ethnic, racial origin, political opinions, religious or philosophical beliefs, trade union memberships or sexual activities) is only allowed with your consent OR if there is a serious and imminent threat to a person's life or health.

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. How we apply this principle

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
- some research purposes, subject to approval by a Human Research Ethics Committee,
- 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, or
- for some law enforcement and investigative purpose

12.5. Other relevant points

The NSW Privacy Commissioner's guide *Privacy and People with Decision-making Disabilities* 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* 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.

In certain scenarios the Information Protection Principles and Health Privacy Principles do not apply

The IPPs and HPPs do not apply in certain situations or to certain information collected. Further details are provided in Appendix 3. Some of the key situations where collection, use or disclosure of information is exempted the compliance with certain IPPs and HPPs include:

- unsolicited information, unless we have retained it for a purpose (although we will generally treat unsolicited information in the same manner as information we have requested from you)
- personal information collected before 1 July 2000 (although we will generally treat this information in the same manner as information collected after 1 July 2000)
- health information collected before 1 September 2004 (although we will generally treat this information in the same manner as information collected after 1 September 2004)
- law enforcement and investigative purposes and some complaints handling purposes
- when authorised or required by a subpoena, warrant or statutory notice to produce
- if another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- in the case of health information, to lessen or prevent a serious threat to public health or public safety
- some research purposes
- in the case of health information, compassionate reasons, in certain limited circumstances
- finding a missing person
- information sent between public sector agencies to transfer enquiries or to manage correspondence from a Minister or member of Parliament.

The Australian Criminal Intelligence Commission

Where necessary, Service NSW also undertakes police checks with the Australian Criminal Intelligence Commission. In undertaking these checks, we ensure that all personal information collected and received for the purposes of police checks are managed in accordance with our privacy obligations as well as contractual obligations we have with the ACIC.

Statistical information

We will use statistical information based on the personal information gathered from our customers and staff for analysis, policy formulation, and process and service improvement. If this data is used outside of the business unit which collected it, we ensure it is de-identified so that no person can be recognised through the data.

Sometimes we will publish statistical information on our websites. Whenever this is done, again the

information is de-identified. For example, we publish data on the number of speeding fines issued by both the NSW Police or fixed speeding cameras. The number and value of the fines is aggregated, and no names or addresses are included, so that when another person is looking at the data, they cannot work out who it is referring to.

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 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*
- Service NSW *Information Security Policy*

PART F: How to Access and Amend Personal Information

In the majority of cases, you have the right to access and amend the personal and health information we hold about you, for example, if you need to update your contact details.

Service NSW must provide access to or amend personal or health information without excessive delay or response. We do not charge any fees to access or to amend personal or health information, unless you are lodging a formal application under the *Government Information (Public Access) Act 2009* (GIPA Act) (see below).

Formal and Informal Requests

Informal Requests

An informal request simply means that you contact the relevant business unit within Service NSW, or the Service NSW Privacy Officer, and ask for the information you are seeking. There are no fees required and no formal requirements to be met.

You are encouraged to contact the relevant division or business unit with Service NSW directly if you are trying to access or amend your information. You can also contact: governanceandrisk@service.nsw.gov.au.

In many cases, the relevant business unit will be able to amend your personal or health information informally, but will often require something in writing from you to ensure the security and accuracy of the information being amended.

Formal Requests

Formal requests to access personal or health information can be made under the PPIP Act, HRIP Act or the GIPA Act, depending on the circumstances and the sensitivity of the information involved. You would generally need to complete a particular form and provide specific details before your application will be valid. You can find out about making formal access applications under GIPA via our website.

No fee is required if you are requesting information under the PPIP or HRIP Acts, however GIPA applications will require the application fee to be paid.

Formal requests for your personal or health information (whether you are a member of the public or a staff member) should be sent to governanceandrisk@service.nsw.gov.au

The Office of the Privacy Commissioner, within the Information and Privacy Commission (IPC), can also provide help and guidance about your rights around your personal and health information (see Part 6 for how to contact the IPC).

Limits on accessing or amending other people's information

We are usually restricted from giving you access to someone else's personal and health information. While the PPIP Act and the HRIP Act give you the right to access your own information, the Acts generally do not give you the right to access someone else's information.

However both the PPIP and HRIP Acts allow you to give us permission to collect your personal and health information from, and disclose it to, someone else.

If you do require someone to act on your behalf, you will need to give us your written consent. The IPC's guide to *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.

If you are under 16 we are allowed to collect information directly from your parents or guardian.

The PPIP and HRIP Acts enable us to disclose your information to another person in limited circumstances, such as to prevent a serious and imminent threat to the life or health and safety of an individual. In the case of health information, other reasons include finding a missing person or for compassionate reasons in certain limited circumstances.

The GIPA Act may also allow your personal information to be provided to others if the public interest considerations in favour of disclosure outweigh the public interest considerations against disclosure. Each decision under the GIPA Act is made on a case by case basis and must take into account the fact that personal information will be revealed, as well as any breach of the IPPs and HPPs, as public interest considerations against disclosure.

PART G: Privacy complaints

If you have any concerns about the way your personal or health information has been handled, or you disagree with the outcome of your request to access or amend your personal or health information, you have the right to both an internal review of the decision by Service NSW or external review by the IPC or NCAT, depending on the situation.

Any person may make a complaint:

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

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

General Principles

If you have a complaint about the way your personal or health information has been handled, or disagree with the outcome of your application to access and/or amend your personal and health information, we encourage you to discuss any concerns with the staff member or division dealing with your information (if known). You can also contact the Service NSW Privacy Officer by phone on 13 77 88 or by email at governanceandrisk@service.nsw.gov.au.

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'.

Requirements

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.

To help you apply for an internal review, you can use the application form from the IPC. This can be downloaded from their website at www.ipc.nsw.gov.au. Although we encourage use of the form, it is not compulsory. You may submit any other relevant material along with your application.

What you can expect from us

- Your application will be acknowledged in writing and the acknowledgement will include an expected completion date;
- 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;
- 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
- The internal review will be completed within 60 days of receiving your application and we will inform you of the outcome of the review within 14 days of completing it. If the review is not completed within this time, you have the right to seek external review at the NSW Civil and Administrative Tribunal (NCAT).
- We will follow the Privacy Commissioner's Internal Review Checklist (available at ipc.nsw.gov.au) and give consideration to any relevant material submitted by you and/or the Privacy Commissioner.
- A copy of the written complaint will be provided to the Privacy Commissioner
- The Privacy Commissioner may make submissions to Service NSW as part of the internal review process;
- In making a decision, we may decide to:
    - take appropriate remedial action
    - make a formal apology to you
    - implement administrative measures to ensure that the conduct will not occur again
    - undertake to you that the conduct will not occur again, and/or

- take no further action on the matter.

- You will be informed of the outcome within 14 days of the internal review being decided, including:
  - the findings of the review
  - the reasons for those findings
  - the action DCS proposes to take
  - the reasons for the proposed action (or no action), and
  - your entitlement to have the findings and the reasons for the findings reviewed by NCAT.

Role of the NSW Privacy Commissioner

The PPIP Act requires that the Privacy Commissioner be informed of the receipt of an application for an internal review of conduct and receive regular progress reports of the investigation. In addition, the Commissioner is entitled to make submissions about the application for internal review.

When we receive your application, we will provide a copy to the Privacy Commissioner. We will then continue to keep the Privacy Commissioner informed of the progress of the internal review, the findings of the internal review and the proposed action to be taken by us in response to the internal review. Any submissions made by the Privacy Commissioner to us will be taken into consideration when making our decisions

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 H: Strategies for implementing and reviewing this Plan

Service NSW's first Privacy Management Plan was drafted in early 2013 and has been reviewed appropriately since.

This edition is a comprehensive review undertaken in July 2019.

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.

Promoting this Plan

Public Awareness

The plan is a commitment of service to our stakeholders of how we manage personal information and health information. As it is central to how we do business, we have made this plan easy to access and easy to understand for people from all kinds of backgrounds.

Additionally, we are required to make this plan publicly available as open access information under the *GIPA Act.*

We will publish this plan on our website in a format that is accessible to the widest possible audience, regardless of technology or ability.

Service NSW Executive

Our executive team is committed to transparency about how we comply with the PPIP Act and HRIP Act, which is reinforced by:

- endorsing the plan and making it publicly available
- reporting on privacy in our annual report in line with the *Annual Reports (Departments) Act 1985* and *Annual Reports (Departments) Regulation 2015*; and
- using the plan as part of induction for new employees, agents and contractors.

Service NSW Employees

We make sure our staff are aware of this plan and how it applies to the work they do by:

- training staff so they understand their privacy obligations and how they are to manage personal and health information
- providing targeted training for those staff who work in areas with a higher exposure to the personal and/or health information of customers or staff, such as those who perform human resources functions, staff who process applications and claims, frontline counter and phone staff, and dispute resolution officers
- providing refresher training so that staff maintain awareness of privacy in doing their daily

business

- writing this plan in a practical way so our staff can understand what their privacy obligations are, how to manage personal and health information in their work and what to do if unsure about their privacy obligations
- publishing this plan together with any subordinate plans or Codes of Practice on our intranet, and
- highlighting the plan at least once a year (for example, during Privacy Awareness Week).

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

PART I: Contacts

Service NSW Privacy Officer

Governance & Risk

Service NSW

GPO Box 7057

Sydney NSW 2001

Phone: 13 77 88

Email: governanceandrisk@service.nsw.gov.au

The Information and Privacy Commission (IPC)

The NSW Privacy Commissioner's contact details are:

Phone: 02 9619 8672

Email: ipcinfo@ipc.nsw.gov.au

Web: www.ipc.nsw.gov.au

Mail: PO Box R232 Royal Exchange NSW 2001

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

The Information and Privacy Commission (IPC)

NCAT's contact details are:

Phone: 1300 006 228 and select Option 3 for all Administrative and Equal Opportunity Division enquiries

Web: www.ncat.nsw.gov.au

Post: NSW Civil & Administrative Tribunal, Administrative and Equal Opportunity Divisions, GPO Box 4005, Sydney NSW

PART J: Appendices

Appendix 1: Information Protection Principles and Health Privacy Principles
Appendix 2: Other Related Laws
Appendix 3: Exemptions
Appendix 4: Guide to Drafting Privacy Notices

Appendix 1: Information Protection Principles and Health Privacy Principles

The Information Protection Principles (IPPs) explained for members of the public (IPC fact sheet, September 2014)

The 12 Information Protection Principles (IPPs) are your key to the *Privacy and Personal Information Protection Act 1998* (PPIP Act)

These are legal obligations which NSW public sector agencies, statutory bodies, universities and local councils must abide by when they collect, store, use or disclose personal information. As exemptions may apply in some instances, it is therefore suggested you contact the Privacy Contact Officer at the agency or the Information and Privacy Commission NSW (IPC) for further advice.

Collection

1. Lawful

An agency must only collect personal information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.

2. Direct

An agency must only collect personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.

3. Open

An agency must inform you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.

4. Relevant

An agency must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

5. Secure

An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

Access and accuracy

6. Transparent

An agency must provide you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency must allow you to access your personal information without excessive delay or expense.

8. Correct

An agency must allow you to update, correct or amend your personal information where necessary.

Use

9. Accurate

An agency must ensure that your personal information is relevant, accurate, up to date and complete before using it.

10. Limited

An agency can only use your personal information for the purpose for which it was collected unless you have given consent, or the use is directly related to a purpose that you would expect, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

11. Restricted

An agency can only disclose your information in limited circumstances if you have consented or if you were told at the time they collected it that they would do so. An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

12. Safeguarded

An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

The Health Privacy Principles (HPPs) explained for members of the public (IPC fact sheet, May 2014)

The 15 Health Privacy Principles (HPPs) are the key to the *Health Records and Information Privacy Act 2002* (HRIP Act).

These are legal obligations which NSW public sector agencies and private sector organisations must abide by when they collect, hold, use and disclose a person's health information. Exemptions may apply, therefore it is suggested you contact the Privacy Contact Officer or the Health Information Manager in the organisation or agency in the first instance. Or contact the Information and Privacy Commission NSW (IPC) for further advice.

Collection

1. Lawful

An agency or organisation can only collect your health information for a lawful purpose. It must also be directly related to the agency or organisation's activities and necessary for that purpose.

2. Relevant

An agency or organisation must ensure that your health information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

3. Direct

An agency or organisation must collect your health information directly from you, unless it is unreasonable or impracticable to do so.

4. Open

An agency or organisation must inform you of why your health information is being collected, what will be done with it and who else might access it. You must also be told how you can access and correct your health information, and any consequences if you decide not to provide it.

Storage

5. Secure

An agency or organisation must store your personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and accuracy

6. Transparent

An agency or organisation must provide you with details regarding the health information they are storing, why they are storing it and what rights you have to access it.

7. Accessible

An agency or organisation must allow you to access your health information without unreasonable delay or expense.

8. Correct

Allows a person to update, correct or amend their personal information where necessary.

9. Accurate

Ensures that the health information is relevant and accurate before being used.

Use

10. Limited

An agency or organisation can only use your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 10 applies). Otherwise separate consent is required.

Disclosure

11. Limited

An agency or organisation can only disclose your health information for the purpose for which it was collected or a directly related purpose that you would expect (unless one of the exemptions in HPP 11 applies). Otherwise separate consent is required.

Identifiers and anonymity

12. Not identified

An agency or organisation can only give you an identification number if it is reasonably necessary to carry out their functions efficiently.

13. Anonymous

Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

Transferrals and linkage

14. Controlled

Only transfer health information outside New South Wales in accordance with HPP 14.

15. Authorised

Only use health records linkage systems if the person has provided or expressed their consent.

Appendix 2: Other related laws

This section contains a summary of other laws that may impact the way we handle personal and health information.

Government Information (Public Access) Act 2009 (GIPA Act)* and *Government Information (Public Access) Regulation 2009

Under this law people can apply for access to government information we hold. Sometimes this information may include personal or health information. The Act contains public interest considerations against disclosure of information that would reveal an individual's personal information or contravene an information protection principle or health privacy principle under the PPIP and HRIP Acts.

If a person has applied for access to someone else's personal or health information we will usually consult with the affected third parties. If we decide to release a third party's personal information despite their objections, we must not disclose the information until the third party has had the opportunity to seek a review of our decision.

When accessing government information of another NSW public sector agency in connection with a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure.

For more information on the operation of the GIPA Act and your personal information, please contact DCS's Ministerial Services team (see Part 6 for how to contact us).

General Data Protection Regulation (GDPR)

Although a European privacy law, the GDPR is designed to have extra-territorial reach. The GDPR came into effect 25 May 2018 and applies to any organisation offering goods or services to, or monitoring the behaviour of, individuals living in the European Union (EU). This could include some NSW public sector agencies, or vendors and suppliers to NSW public sector agencies.

Government Information (Information Commissioner) Act 2009 (GIIC Act)

Under this law the Information Commissioner has the power to access government information held by other NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint

under the GIPA Act and GIIC Act. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission.

For further information on the operation of the GIIC Act, contact the IPC (see Part 6 for how to contact the IPC).

Data Sharing (Government Sector) Act 2015 regarding the sharing of government data between government agencies and the government Data Analytics Centre, including the sharing of de-identified personal data. Enhanced privacy safeguards apply and the usage of personal and health information must be in line with current privacy legislation.

Crimes Act 1900 includes offences regarding accessing or interfering with data in computers or other electronic devices.

Independent Commission Against Corruption Act 1988 regarding the misuse of information.

Public Interest Disclosures Act 1994 **(PID Act)** regarding disclosing information that might identify or tend to identify a person who has made a public interest disclosure.

State Records Act 1998 and State Records Regulation 2015 regarding the management and destruction of records.

Appendix 3: Exemptions

The PPIP and HRIP Acts contain exemptions from compliance with certain IPPs and HPPs.

The main exemptions to each principle are:

Limiting our collection of personal and health information – IPP 1 [PPIP s8] and HPP 1

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- in the case of personal information, for certain Ministerial correspondence or referral of inquiries
- in the case of personal information, to enable the auditing of accounts of performance of an agency or agencies
- in the case of personal information, certain research purposes

How we collect personal and health information – the source – IPP 2 [PPIP s9] and HPP 3

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- in the case of personal information, some law enforcement or some investigative and complaints handling purposes
- where another law authorises or requires us not to comply with this principle
- where non-compliance is otherwise permitted, implied or contemplated by another law
- in the case of personal information, where compliance would disadvantage the individual

Notification when collecting personal and health information – IPP 3 [PIPP s10] and HPP 4

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- the individual concerned has expressly consented to the non-compliance
- some law enforcement and investigative or complaints handling purposes
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- where compliance would disadvantage the individual
- where notification about health information would be unreasonable or impracticable

How we collect personal and health information – the method and content – IPP 4 [PPIP s11] and HPP 2

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- law enforcement or some investigative and complaints handling purposes
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- where compliance would disadvantage the individual

Retention and security – IPP 5 [PPIP s12] and HPP 5

- in the case of health information, the organisation is lawfully authorised or required not to comply
- in the case of health information, non-compliance is permitted under an Act or any other law

Transparency – IPP 6 [PPIP s13] and HPP 6

- if another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law

Access – IPP 7 [PPIP s14] and HPP 7

- some health information collected before 1 September 2004
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- the provisions of the GIPA Act that impose conditions or limitations (however expressed)

Correction – IPP 8 [PPIP s15] and HPP 8

- some health information collected before 1 September 2004
- some investigative or complaints handling purposes
- if another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- the provisions of GIPAA that impose conditions or limitations (however expressed)

Accuracy – IPP 9 [PPIP s16] and HPP 9

- there are no direct exemptions to the operation of this principle

Use – IPP 10 [PPIP s17] and HPP 10

- the individual concerned has consented to the non-compliance
- law enforcement and some investigative or complaints handling purposes
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- in the case of health information, to lessen or prevent a serious threat to public health or public safety
- in the case of health information, finding a missing person
- information sent to other agencies under the administration of the same Minister or Premier for the purposes of informing the Minister or Premier
- some research purposes
- in the case of health information, some training purposes

Disclosure – IPP 11 &12 [PPIP s18 and 19] and HPPs 11 & 14

- law enforcement and some investigative and complaints handling purposes
- when it is authorised or required by a subpoena, warrant or statutory notice to produce
- if another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law
- in the case of health information, to lessen or prevent a serious threat to public health or public safety
- in the case of health information compassionate reasons in certain limited circumstances
- finding a missing person
- information sent to other agencies under the administration of the same Minister or Premier for the purposes of informing the Minister or Premier
- in the case of health information, some research and training purposes

Identifiers – HPP 12

- There are no direct exemptions to the operation of this principle.

Linkage of health records – HPP 15

- health information collected before 1 September 2004
- where another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or contemplated by another law

Appendix 4: 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