Service NSW Privacy Management Plan

April 2026

NSW GOVERNMENT

Service NSW

Acknowledgement of Country

Service NSW acknowledges the Traditional Custodians of the lands where we work and live. We celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

We pay our respects to Elders past and present and acknowledge the Aboriginal and Torres Strait Islander people that contributed to the development of this Policy.

We advise this resource may contain images, or names of deceased persons in photographs or historical content.

Service NSW Privacy Management Plan

Published by Service NSW

service.nsw.gov.au

Contents

1 Privacy Management Plan overview

1.1 Purpose

The Service NSW Privacy Management Plan (PMP) sets out our commitment to respecting the privacy rights of our customers and staff. It describes the main types of personal and health information we handle to conduct our legislative functions and activities under the *Service NSW (One-stop Access to Government Services) Act 2013* (Service Act) and explains how we protect that information throughout its lifecycle.

The privacy of our customers, employees and others for whom we handle personal, or health information is protected under either:

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

The PMP provides practical guidance for how Service NSW protects personal and health information and meets the requirements of section 33 of the PPIP Act. The PMP also includes mechanisms for individuals understand how to gain access to and amend their information, and to resolve privacy-related complaints.

1.2 What the plan covers

Section 33 of the PPIP Act requires all NSW Government agencies, including Service NSW to have a PMP. The PMP provides information on:

- how we develop privacy policies and practices
- how we share these policies and practices within the organisation and train staff to use them
- our processes for privacy internal reviews under Part 5 of the PPIP Act
- how we meet our obligations and responsibilities set out in Part 6A of the PPIP Act for the mandatory notification of data breaches
- other matters that Service NSW considers relevant to the protection of personal and health information.

1.3 Communicating the PMP

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

- writing this plan in a practical way so our staff can understand their privacy obligations, how to manage personal and health information in their work and what to do if they are unsure about their privacy obligations
- training staff on their privacy obligations and how to manage personal and health information through mandatory, privacy specific training — on commencement and yearly refresher training
- providing targeted training for staff who work in areas with a higher exposure to personal and/or health information

- publishing this plan together with any related policies, procedures or codes of practice on the Service NSW intranet site
- highlighting the plan during privacy awareness week and at other times during the year.

1.4 Our commitment

This PMP is Service NSW's commitment to our customers and staff on how we manage personal and health information. We review and update this PMP as required to ensure ongoing compliance with applicable privacy laws and to address any changes in processes, procedures, or other activities we undertake. This edition is a review undertaken in March 2026.

This PMP is published and made available on the Service NSW website here.

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 on 13 77 88, or by email to privacy@service.nsw.gov.au.

2 About Service NSW

Service NSW is an NSW Government executive agency related to the Department of Customer Service (DCS). We make it easier for people and businesses across NSW to access government services by working in partnership with NSW, Commonwealth and state and territory agencies, and private organisations.

We exercise customer service functions on behalf of many government agencies, local government and some private sector organisations. For example, we support high volume transactions for agencies such as Transport for NSW, Fair Trading NSW, Liquor and Gaming, and Births Deaths and Marriages.

We also support transactions that may not be a customer service function but do relate to the delivery of NSW Government services. These functions are provided to Service NSW under Ministerial Direction, which is explained in more detail in the following section.

Service NSW supports customers through a multi-channel model of service delivery. We provide:

- a single NSW Government phone number and contact form
- a MyServiceNSW Account portal to connect with NSW Government services
- Service Centres for over-the-counter transactions
- Service NSW apps to easily access NSW Government services on mobile devices.

2.1 Legislative functions and transactions

Part 2 of the Service Act sets out Service NSW's legislative functions, including customer service functions conferred by an agreement or delegated to the Head of Agency by government agencies, local government, and prescribed non-government entities.

The Service Act also outlines that the Minister for Customer Service and Digital Government (the Minister) can direct Service NSW to perform any other functions relating to the delivery of government services to the people of New South Wales.

2.1.1 Customer service functions

Service NSW primarily delivers customer service functions on behalf of partner agencies. We exercise these functions through delegation or a customer service agreement made under sections 7–10 of Service NSW Act. We have agreements with approximately 60 partner agencies to facilitate support for services and transactions to the NSW community. A list of these agencies is provided in the **Appendix C** to this plan.

Under the Service Act, a customer service function may include activities such as:

- accepting applications or fees related to authorities[1].
- issuing authorities, and other functions related to those authorities
- providing advice or information about government services, laws or any other matter
- receiving payments or claims for payments or making payments (e.g. grants, rebates)
- collecting and managing personal and health information in line with privacy laws.

[1] Under the Service Act an authority means 'a licence, permit, approval or any other authorisation'.

2.1.2 Functions provided by ministerial direction

Section 4(c) of the Service Act, outlines that the Minister may direct Service NSW to perform other functions relating to the delivery of government services to the people of New South Wales.

Functions we have been directed to perform include, but are not limited to:

- providing vouchers, grants and rebates to provide relief or stimulate the economy and assist in the recovery from events such as natural disasters
- enabling people to use their MyServiceNSW account or credentials to streamline accessing other NSW Government services, prove their identity and receive notifications about services from their account
- undertaking fraud prevention, detection, and investigation to assess the integrity of personal information provided for MyServiceNSW accounts and applications for grants, rebates or other benefits administered by Service NSW, and
- providing the means for customers to apply for, create, hold and use an NSW digital identity and other credentials in the form of verifiable credentials.

You can contact the Information Access Team for more information about current ministerial directions in place. Visit the Service NSW Information Guide for more information.

2.1.3 Transactions we perform

Examples of transactions performed by Service NSW on behalf of our partner agencies or under a Ministerial Direction include:

- accepting applications for and processing licenses, permits and authorities; for example, driver licences, car registrations, boating and fishing licences on behalf of Transport for NSW as well as other agencies that manage licences or credentials such as Liquor and Gaming
- receiving applications or requests for replacement certificates or other documents issued by the Registrar of Births, Deaths, and Marriages
- managing rebates such as Toll Relief and IVF Rebates
- delivering vouchers such as the Active and Creative Kids vouchers
- providing guidance and business advisory services to NSW businesses
- delivering a range of grants on behalf of the NSW Government to support businesses and individuals affected by disasters or emergencies
- disaster preparation and recovery services and coordination, working in partnership with the Department of Communities and Justice and NSW Reconstruction Authority
- receiving fines and taxes on behalf of Revenue NSW
- applications for Fair Trading, Building Commission, and Safe Work permits, certificates, and authorities
- processing applications for Working with Children Checks and National Disability Insurance Scheme Worker Checks for the Office of the Children's Guardian
- booking appointments to assist individuals to access government services or savings they may be eligible for.

2.2 Customer service channels

2.2.1 MyServiceNSW Account and the Service NSW App

Customers can use their MyServiceNSW Account to connect online with NSW Government services, quickly and securely. This includes to:

- check and renew licences and registrations
- apply for vouchers, rebates and other assistance
- perform online transactions with Service NSW or our partner agencies, including identity verification
- switch to digital notifications for services and updates
- create a business profile
- find details about services without having to call or wait in line.

Each transaction performed using a MyServiceNSW account will have its own privacy collection notice outlining how we manage personal information for that transaction. These are provided during the transaction, and a copy of collection notices is available on the Service NSW website.

Customers can also use their MyServiceNSW Account to log into the Service NSW App to access a range of government services and information. This includes:

- push notifications containing important information
- digital licences
- vehicle registration checks and renewals
- fines and demerits
- licence or credential verifier
- vouchers
- Seniors/Senior Savers Card.

2.2.2 Frontline service delivery

Customers can visit or call one of our Service NSW teams to conduct partner agency transactions over the phone or in-person if they prefer.

We have a presence across NSW, supported by 1186 Service Centres, three Driver Testing Centres, 33 Council Agencies, four Mobile Service Centres including the Kangaroo service which visit more than 40 rural and remote Aboriginal communities, five Contact Centres and four Middle Offices.

Partner agencies provide their own privacy collection notice when transactions are performed using a physical form or in person at a Service Centre. You can find more information about our frontline service delivery locations by visiting https://www.service.nsw.gov.au/service-centre

3 Roles and Responsibilities

3.1 Staff responsibilities

All Service NSW staff are required to comply with the PPIP Act and HRIP Act. Non-compliance with these Acts may result in potential risk of harm to customers, as well as a loss of customer trust, reputational damage, and financial costs such as compensation.

3.1.1 Offences under the PPIP and HRIP Acts

Both Acts[2] also contain offence provisions applicable to staff who use or disclose personal information or health information without authority. The maximum penalty is up to two years' imprisonment, or a $11,000 fine, or both. This means that it is an offence to:

- intentionally use, disclose, or offer to supply personal or health information about another person except when permitted in their role
- offer to supply personal or health information for an unauthorised purpose
- attempt to persuade, threaten, intimidate, etc., a person to refrain from making a request for their health information, a privacy complaint about their health information, or an internal review about their health information
- hinder the Privacy Commissioner or member of staff doing their job.

All Service NSW staff have a responsibility to report incidents or behaviours that could compromise our trusted position to manage customer personal information.

If you see something suspicious, including if someone may be committing an offence above, please make an anonymous or confidential report by using the DCS Integrity Hotline.

3.2 The Service NSW Privacy Officer and privacy team

Service NSW has a dedicated privacy team to help staff understand their obligations when dealing with personal and health information. The Service NSW Director Privacy and Fraud is the designated Privacy Officer and leads a team of privacy managers and advisors. The Privacy Officer's responsibilities include:

- publishing the PMP and ensuring it remains up to date by reviewing the plan quarterly
- informing staff of changes to the PMP
- making material available to staff to help them understand their privacy obligations, and how to manage personal and health information in their work
- providing privacy expertise and assurance on the development of new products and services, and to existing products and services as they evolve

[2] See s 62 of the PPIP Act, s 68 and s 70 of the HRIP Act, and s 308H of the Crimes Act 1900

- recommending controls to help manage privacy risks, and providing privacy expertise to assist their implementation
- responding to privacy incidents and data breaches
- publishing information on our compliance with the PPIP Act and HRIP Act and other information as required under NSW Government annual reporting obligations
- handling privacy complaints
- maintaining reporting on privacy incidents, complaints, and other relevant metrics
- providing privacy training and awareness activities to Service NSW employees, contractors, and service providers
- being available to answer any questions Service NSW employees may have about their privacy obligations.

The Privacy Officer is accountable for ensuring the delivery of privacy functions, but delegates responsibilities to the Service NSW privacy managers and/or the privacy team. The privacy team also works with privacy officers in DCS and partner agencies, where appropriate.

You can contact the Service NSW Privacy Officer at:

Enterprise Risk and Enablement Division, Service NSW
GPO Box 7057, Sydney NSW 2001
Phone: 13 77 88
Web: www.service.nsw.gov.au/privacy
Email: privacy@service.nsw.gov.au

3.3 Service NSW Executive

Our Executive team is committed to transparency and ensuring Service NSW complies with our privacy obligations under the PPIP Act and HRIP Act. We reinforce this by:

- endorsing the PMP and making it publicly available
- reporting on privacy in our annual report in line with the *Government Sector Finance Act 2018*, the *Government Sector Finance Regulation 2024*, and the TPG25-10 Framework for Financial and Annual Reporting
- ensuring the PMP is part of induction for new employees, agents, and contractors
- using the PMP as an everyday reference point for our privacy management practice.

4 Strategies to comply with privacy laws

4.1 Privacy policies and practices

The Service NSW privacy team has developed a range of policies and guidance material to ensure compliance with privacy legislation, and to protect the personal information we collect, hold, use, and disclose.

We develop and review our policy, processes, and guidelines by:

- monitoring changes in the legislative, policy and operational environment for impacts on our privacy management
- conducting regular reviews of privacy policies and practices, including this PMP
- considering the privacy implications of complaints, internal reviews, or privacy breaches
- implementing changes to organisational policies or systems.

We communicate our policies and practices, including this PMP, through mandatory privacy training, targeted training and awareness sessions and the publication of information through a dedicated Service NSW Privacy intranet page.

We also adopt certain policies of DCS such as the DCS Information Security Policy, the ICT Acceptable Use Policy, and the Code of Ethics.

You can find a full list of Service NSW and DCS policies that impact how we manage personal information in **Section 8.**

Service NSW staff can find the full range of privacy policies, standards, and guidelines on our Privacy intranet page here.

You should read these before taking any action that may involve our customer's personal information and contact the Privacy Officer if you have any questions about the policies.

4.2 Privacy assurance and advice

Service NSW takes a collaborative approach to managing privacy. Good risk management, information security and information management practices support our compliance with our privacy obligations.

Service NSW implements best practice privacy by design principles, proactively embedding privacy management into plans, policies and frameworks that guide our business practices and customer service delivery.

4.2.1 Privacy by design

'Privacy by design' is a set of key principles that embed good privacy practices into the way products or services are designed. This includes building privacy into the design specifications and architecture of new systems and processes Service NSW implements.

We generally use Privacy Assurance Forms (PAFs) and Privacy Impact Assessments (PIAs) to operationalise the privacy by design principles for projects, systems and service delivery changes that involve new or changed ways of handling personal information.

4.2.2 Privacy impact assessments

At a minimum Service NSW requires a PIA to be conducted for all projects with a high privacy risk. A project may be a high privacy risk if Service NSW considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals or the trust of our customers, employees and stakeholders. The PAF process will help you determine if your project meets this threshold.

A PIA documents a complete overview of the flow of personal or health information in a project or initiative, including the involvement of any third parties and systems that might manage the information on our behalf. A PIA looks at how personal information will be managed to determine whether the project or initiative complies with privacy laws and meets community expectations.

PIAs allow Service NSW to:

- assess whether the deliverables of a project or initiative are compliant against privacy law and in line with community expectations
- identify any privacy risks and make recommendations to control those risks.
- ensure standardised, consistent, and comprehensive privacy assurance processes are applied to all initiatives
- engender trust in SNSW products and its privacy practices.

Service NSW staff can find details regarding PAFs and PIAs on our Privacy intranet page here.

Staff should always contact the privacy team when developing a new product or service that handles personal information, or when changing existing information handling practices to make sure the privacy team provides assurance and advice.

4.3 Mandatory notification of data breach (MNDB) scheme

The MNDB came into effect on 28 November 2023 following amendments to the PPIP Act. In the event of an eligible data breach the MNDB scheme requires Service NSW to notify the NSW Privacy Commissioner immediately and affected individuals as soon as we can.

A data breach occurs when:

- there is unauthorised access to, or disclosure of personal information held by Service NSW, OR
- personal information held by Service NSW is lost in circumstances where unauthorised access or disclosure of the information is likely to occur.

Under the MNDB scheme, an eligible data breach is where:

- a data breach has occurred, AND
- a reasonable person would conclude that the access or disclosure of the personal information would be likely to result in serious harm to an individual to whom the compromised personal information relates.

Service NSW publishes a Data Breach Policy which documents how we respond to an eligible data breach. This is available on the Service NSW website.

Service NSW has also developed a Data Breach Response Plan for internal use, available on the privacy intranet page. This document guides staff on the data breach response process, including:

- what to do when there has been a data breach or suspected data breach
- how to mitigate potential harm to affected individuals
- when and how to notify the Privacy Commissioner.

If it is not possible or reasonably practicable for Service NSW to notify affected individuals, we will take reasonable steps to publish a public notice on the Service NSW website. All data breaches involving a public notification will be maintained on the Service NSW Data Breach Notification register for at least 12 months.

Contact the Service NSW privacy team immediately if you become aware of a suspected eligible data breach.

Service NSW staff can find more information and resources on how to manage potential privacy breaches, including the operation of the MNDB scheme by visiting the Privacy intranet page here.

4.4 Staff training and awareness

The Service NSW privacy team develops and delivers an annual privacy training program which is a key control in preventing and preparing staff to contain privacy breaches.

The program is designed to raise staff awareness of privacy law and the importance of protecting personal information. This is done by delivering one or more of the following activities:

- mandatory e-learning modules for all staff
- tailored sessions to business units
- privacy workshops
- open sessions with the privacy team
- Privacy Awareness Week (PAW) activities
- short educational Privacy videos.

The privacy team publishes a range of educational videos and guidance material to support staff to build privacy awareness.

Staff can find more information and resources on by visiting the Privacy intranet page here.

4.5 Privacy maturity and monitoring

Service NSW is committed to continually improving its privacy governance, processes and procedures. The privacy team assesses Service NSW's privacy maturity against five elements that are commonly used as part of the methodology for determining the maturity of an organisation's privacy management:

- Governance and Culture
- Privacy Strategy

- Privacy Processes
- Privacy Risk and Assurance
- Data Breach Response.

Based on the assessment, we document recommended actions in a Privacy Management Action Plan (PMAP), with the goal to improve privacy maturity across the agency for the year/s ahead through a range of activities.

4.6 SNSW use of Artificial Intelligence

Artificial Intelligence (AI) is the ability of a computer system to perform tasks that would normally require human intelligence, such as learning, reasoning, and making decisions. An automated decision making (ADM) system describes a computerised process, which may or may not involve the use of AI, that either assists or replaces the judgement of human decision-makers. Either fully or partially, it may:

- make a final decision
- make a recommendation to a decision-maker
- guide a human decision-maker through a decision-making process
- provide decision support, e.g., commentary at relevant points in the decision-making process
- provide preliminary assessments.

There is some AI functionality embedded in Service NSW's enterprise protected third-party tools such as Microsoft Copilot. Although there is a risk that staff may enter personal information into these tools, the risk is reduced through standards, security and organisational guidelines and resources, and privacy awareness campaigns. A dedicated 'Using AI at Service NSW' and 'AI Assurance at Service NSW' intranet site has been developed to help guide staff.

Service NSW requires an AI self-assessment for all initiatives that design, develop, deploy, procure, or use systems containing AI components and review by data governance and privacy teams. This applies across all project stages and the solution lifecycle and is a continuous process. The process is based on the Digital NSW Artificial Intelligence Strategy and AI Ethics Policy, and Service NSW mandates the NSW Government Artificial Intelligence Assessment Framework.

The Service NSW Data and AI Governance Committee oversees all AI initiatives with medium or high risks, or where we share large datasets with another agency. All initiatives identified as high risk following the application of all mitigations and controls are referred to the NSW Government AI Review Board. Service NSW AI Assurance Register documents all AI initiatives.

At Service NSW, AI or ADM enhanced processes go through human verification to determine the accuracy of AI output. Current approved AI initiatives use customer and/or staff personal information to:

- analyse complaints to identify themes that enhance frontline services and the customer experience
- improve our disaster recovery functions by analysing customer and staff feedback
- identify and investigate fraudulent applications for grants and rebates
- provide personalised recommendations to customers based on their user profile and transaction history
- assist Contact Centre staff with customer enquiries.

If you are considering using an AI or ADM component in any systems or tools, you must follow the AI Acceptable Use Standard and Procedure. You can find more information on the Standard and Procedure by visiting the Data Governance intranet site here or by contacting the Data Governance team directly.

Staff can also visit the Using AI at Service NSW to understand how to use Artificial Intelligence (AI) in day-to-day work.

5 How Service NSW manages personal and health information

5.1 The PPIP Act and HRIP Act

The PPIP Act and HRIP Act set out how NSW Government agencies must manage personal and health information.

The PPIP Act contains 12 Information Protection Principles (IPPs), and the HRIP Act contains 15 Health Privacy Principles (HPPs) which cover the collection, storage, use, and disclosure of personal and health information, as well as security, access, amendment, and disposal of the information.

This section of the PMP provides:

- a definition the principles based on the *IPC Fact Sheet Information Protection Principles for the Public* and the *IPC Fact Sheet – Health Privacy Principles*
- an explanation of how Service NSW meets the IPPs and HPPs.

An explanation of where an exemption may commonly be applied is provided in **section 6** of this PMP.

This section of the PMP uses plain language and does not cover the full complexity of privacy laws, including all exemptions or circumstances which may apply. For example, we have provided a short definition of each IPP/HPP in italics under the relevant heading. We do this to make the obligations easier to understand.

The PMP is an educational tool, and not legal advice. If in doubt, you should always check the exact wording in the legislation and seek guidance from the Service NSW privacy team.

5.2 Collecting personal and health information (IPPs and HPPs 1-4)

The collection principles govern how NSW Government agencies collect information. Service NSW assesses compliance with the principles when collecting personal and/or health information and takes the necessary action to ensure compliance. We typically do this through a privacy impact assessment or similar privacy assurance to ensure the collection principles are being met.

Service NSW collects personal and health information to provide services on behalf of our partner agencies or to perform functions under a Ministerial Direction. We collect personal information through several different channels:

- over the counter in Service Centres (including at councils and mobile Service Centres)
- through the Service NSW Contact Centres, where we retain phone call records, and a written record of your request including any information or advice staff give you
- through the MyServiceNSW account on the Service NSW website
- through information you provide for online transactions or enquiries (including using the Service NSW app)

- at disaster recovery centres and recovery assistance points when disaster strikes an area in NSW
- when providing business advisory services
- to manage and process complaints or requests for internal review.

The type of personal and health information we may collect depends on the transaction or service we are providing. When exercising our functions on behalf of a partner agency, that agency will define the personal information we collect.

Customer personal information we collect and hold includes:

- identity, demographic and contact data such as name, address, telephone number and email address, date of birth, gender, and signature
- financial and other eligibility information related to grants applications
- requests for interpreter services or other accessibility requirements
- business information that may also be personal information
- information related to a disaster that has affected individuals.

We collect limited health information through the types of services we support. The main types of health information we collect, and hold includes:

- some information about physical or mental health or a disability that is required as part of an application for licences, permits and other authorities
- identity, demographic and contact data such as name, address, telephone numbers and email address, date of birth, gender and signature – where collected on behalf of a partner agency that may provide a health service
- information related to health-based grants such the Fertility Rebate Program.

Service NSW also collects staff personal and health information as part of the recruitment process. We have a shared corporate service arrangement for human resources with DCS, who collects the information on our behalf when assisting us to provide human resources functions.

During the recruitment process and throughout employment, we collect information from staff members for reasons such as leave management, workplace attendance, workplace health and safety, and to help Service operate with transparency and integrity.

5.2.1 Lawful collection IPP1 and HPP1

Service NSW must only collect your personal or health information for a lawful purpose. It must be directly related to our functions or activities and necessary for that purpose.

Service NSW meets these principles by ensuring any personal and health information is collected for a lawful purpose and is directly related to our functions and activities under the Service Act. Often the types of personal information collected in our frontline and digital channels are defined for us by our partner agencies. We enter into an agreement with a partner agency before we provide a service on its behalf, or where a service is delivered under a Ministerial Direction.

Agreements go through a rigorous drafting, review, sign-off, and compliance and governance process. This ensures we only ask for personal information that we need to exercise a function under the Service Act for that agency.

5.2.2 Direct collection IPP2 and HPP3

Service NSW must collect personal and health 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.

We will generally collect personal and health information directly from an individual. For example, Service NSW meets these principles by requiring individuals to establish their own MyServiceNSW Account when transacting with us digitally. We also require the individual to provide their own personal information when completing a transaction through one of our assisted channels, such as the Contact Centre or the Service Centre.

We may collect information from third parties under the following circumstances:

- When you have authorised someone else to provide your information. In these cases, we have processes in place to ensure authorisation has occurred. For example, requiring the third party to declare they have authorisation as part of the transaction.
- Where the information relates to a person who is under the age of 16 years. In this case, we may collect the information from a parent or guardian of the person.
- Where a person aged 16 or over has limited capacity (e.g. because of mental illness, intellectual disability, dementia, brain injury, illness, accident or disease).
- Where, in the case of health information, it is unreasonable or impractical to collect the information directly.
- Where an exemption applies (see **section 6** of this PMP).

5.2.3 Open and transparent collection IPP3 and HPP4

Service NSW must inform you that we are collecting your information, the reason or purpose for collecting it, and who will be storing and using it. We must tell you 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.

We have standardised our privacy notice format to ensure that customers are provided with consistency whenever we collect personal or health information. Our standard collection notices contain the following sections:

- why we are collecting your personal information
- if we are collecting your personal information on behalf of a partner agency
- the types of personal information we collect
- how we will use and disclose your information
- whether you are required by law to provide us with your information
- how to contact us and how to access and correct your information.

Service NSW adopts a layered approach to privacy notices, as endorsed by the Privacy Commissioner, to avoid overloading customers with too much information. Service NSW generally provides a copy of a privacy notice before we collect personal information. We also publish a copy of the privacy collection notices provided through digital transactions on our website for transparency.

In the case of inbound calls to the Contact Centre, a recorded message will provide customers with a notice and advise that the call may be recorded or monitored unless consent is withdrawn. Contact Centre employees making outbound calls provide the notice themselves.

Where we provide a service on behalf of a partner agency, Service NSW is permitted to refer customers to that agency's privacy collection notice. The agency's privacy notice must contain the

matters that are required to be provided under IPP3/HPP4. Service NSW commonly relies on this exemption in our Service Centre network as we are often required to use the relevant partner agency paper form to collect personal information. This exemption is detailed in **section 6** of this PMP.

The privacy team is responsible for approving all Service NSW collection notices. All staff should contact the Service NSW Privacy Officer regarding any proposals to collect new personal information or to use existing personal information for a new purpose.

5.2.4 Relevant collection IPP4 and HPP2

Service NSW must ensure that the personal information collected is relevant, accurate, complete, up to date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Conducting a privacy impact assessment or similar privacy assurance means that there is a formal mechanism to review the types of person information collected. This process ensures that information collected to support a transaction is relevant and not excessive. We have also implemented processes in transaction flows so that the personal information we are collecting is accurate, complete and up to date. This includes:

- for our online transactions, we provide the opportunity to review information in the relevant form or application before submitting
- if a MyServiceNSW account is used to complete a transaction, we provide the opportunity to update personal information as part of the transaction. For example, confirming that the address stored in the profile is accurate
- we sometimes conduct a proof of identity check using the Document Verification Service to ensure that the information for certain transactions matches the customer's verified identity
- when attending a Service Centre or calling our Contact Centre, we will check information before processing any requests or transactions.

If customers provide us with personal information that we have not requested and do not need, we call this information "unsolicited". Even though Service NSW did not request this type of information, we still have an obligation to comply with the IPPs.

Service NSW privacy team has developed an unsolicited personal information fact sheet that assists staff with any requests to remove unsolicited personal information from our systems. Staff should visit the Service NSW privacy page for more guidance and information on how to action these requests.

5.3 Storing and securing personal and health information (IPP5 and HPP5)

Service NSW provides a multi-channel model for customers to interact with us digitally, over the counter or by phone. Providing this type of service delivery means Service NSW stores personal information in a range of ways. This includes in:

- Service NSW databases and cloud storage solutions that store transaction information we manage end-to-end, such as grants, vouchers and rebates
- our customer relationship management system
- our cloud-based telephony system used by our Contact Centre
- our records management system
- hard copy documents stored in physical storage locations.

Front line and head office staff may access customer information in our systems to perform their day-to-day duties. We ensure that staff access to systems is tightly controlled by applying access controls and reviewing staff access to systems on a regular basis.

For some partner agency transactions, Service NSW does not store customer information. Instead, our staff are provided with access to the partner agency system to support transactions or enquiries. For example, Service NSW is provided:

- read-only access to Lifelink, a system owned by the NSW Registry of Births, Deaths and Marriages
- read/write access to Transport for NSW's DRIVES system to enter information for licence and registration transactions
- Multicultural NSW's Language Link system to upload scanned documents on behalf of customers.

In these circumstances, the partner agency must ensure adequate storage and security is in place, including access controls and reviews.

Similarly, staff from a partner agency may have access to our systems related to the relevant program we are delivering on their behalf. Access is documented in partner agency agreements and is reviewed regularly. We segregate data they have access to, so they only access the personal information they need to perform their functions.

Service NSW partners with Digital NSW (also a part of the Department of Customer Service) to assist us with certain business operations. This includes providing software to enable Service NSW to process customer transactions, such as government licensing in a system known as Licensing NSW, and with the phone software system that is used in our Contact Centre.

5.3.1 Secure storage (IPP5 and HPP5)

Service NSW must take reasonable steps to store personal and health information securely, keep it no longer than necessary, and dispose of it appropriately. We must also protect the information from loss, unauthorised access, use, modification, disclosure and all other misuse.

Service NSW complies with the principles through our privacy assurance and data governance processes, along with security and vendor risk assessments. For information that Service NSW holds, we implement appropriate storage and security controls in compliance with NSW Government and DCS security policies, as well as Service NSW security standards.

Where we are directed to use a partner agency system to provide a customer service function, the agency has a shared responsibility for ensuring that its system has the appropriate security safeguards and retention periods in place.

5.3.1.1 Service NSW system security controls

The Service NSW Cyber Security team has published a range of standards that detail minimum requirements to manage and reduce risk to Service NSW information and systems. Key system security controls are detailed in standards include:

- Access Management Standard for all systems, including roles and responsibilities, access control mechanisms, provisioning and de-provisioning, account management, authentication management, access reviews, and minimum password requirements.
- Cryptography and Key Management Standard including defining requirements (such as algorithms and key lengths) for the use of cryptographic controls within the Service NSW ICT environment for information at rest or in-transit.
- Logging and Monitoring Standard that helps to identity potential security incidents including unauthorised access, system misuse and other suspicious activities.
- System Acquisition, Development, and Maintenance Standard that sets requirements around secure development practices, secure software design, secure code management, security risk assessment, and system acquisition.
- Vendor Management Security Standard that sets requirements within ICT vendor management, including roles and responsibilities, vendor selection, initial and ongoing vendor security risk assessment, vendor contract management, and vendor register.

All staff must comply with the Code of Ethics and Conduct, DCS Information Security Policy, and related DCS IT Security and Acceptable Use Policies when accessing or using Service NSW systems.

There are additional Service NSW security standards that outline minimum requirements when establishing or procuring Service NSW systems.

Please contact the Service NSW Cyber Security team if you are unsure about your security obligations or for more information about the polices and standards you are required to follow.

5.3.1.2 Retention and disposal

Service NSW creates and captures records in accordance with the State Records Act and the DCS Customer Service Records Management Policy.

Records and are a vital asset for information accessibility, government transparency, and institutional trust. They must be kept for a minimum term, as determined by State Records retention and disposal authorities. The authorities identify those records created and received by NSW public offices which are required as State archives and provide approval for the destruction of other records after minimum retention periods have been met.

Service NSW retains personal information in line with the disposal authorities, including the Service NSW Functional Disposal Authority FA425, which is specific to Service NSW functions.

Where we exercise functions for a partner agency, we will dispose of information securely in accordance with retention periods specified by the partner agency or transfer the records to them.

5.3.1.3 Access controls for MyServiceNSW Account information and transactions

Service NSW has implemented a range of reasonable security measures to protect customer personal information in the MyServiceNSW Account and Service NSW App. This includes:

- Mandatory Multi-Factor Authentication for all MyServiceNSW Accounts to help to keep information secure. This means all customers are required to have two factors of authentication and will be required to meet an additional authentication challenge when using their MyServiceNSW Account credentials.

- Real-time notifications are in place to inform our customers when activity related to their MyServiceNSW Account occurs. These notifications enable customers to take immediate action if they are concerned about any unusual Activity
- Requiring customers to verify their identity using proof of identity information to proceed with a particular transaction. Service NSW uses the Commonwealth Document Verification Service (DVS) to check the validity of your proof of identity documents against the records of document issuers.
- For transactions where a stronger level of verification is required, customers may be given the option of verifying their identity using Service NSW's biometric face verification system, including the NSW Digital ID. These are optional; customers may choose to verify in person at a Service Centre instead of using either service.

5.4 Accessing and amending personal or health information (IPPs and HPPs 6-8)

The 'access and accuracy' principles (IPPs and HPPs 6-8) govern how Service NSW is transparent with information it holds, and how you can access the personal or health information Service NSW holds about you.

5.4.1 Transparency IPP6 and HPP6

Service NSW must provide you with details regarding your information we are storing, why we are storing it and what rights you have to access it.

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

Service NSW complies with this principle by publishing this PMP on our website. It sets out the major categories of personal information that we hold and explains our privacy obligations.

A schedule of our partner agencies, with whom we have a shared responsibility for customer personal information, is also attached at **Appendix C**.

5.4.2 Access IPP7 and HPP7

Service NSW must allow you to access your personal or health information without excessive delay or expense.

In most cases, individuals have the right to access and amend the personal and health information we hold about them. For example, if you need to update your contact details. Requests for access to personal information can be made by phone, email or in person. Access to your own information is free.

Where individuals seek access to information we hold about them in relation to a transaction with a partner agency, we may refer them to that agency to process their request, unless the relevant agreement with that partner agency has provided for us to do this on their behalf.

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, unless you have their written consent.

5.4.2.1 Making informal access requests

Informal requests can be made to Service NSW to access or amend information. There is no fee to informally access or amend personal information or health information. The request does not need

to be in writing, but individuals will need to go through a proof of identity check to confirm they are authorised to access the information.

To request access to information:

- contact the area of Service NSW you originally interacted with
- log into your MyServiceNSW Account and amend your profile information
- go to your local Service Centre
- call us on 13 77 88
- message us via the Contact Us form
- contact the Privacy Officer.

Some information we collect that is stored in a partner agency's system may have different access request requirements. For example, certain information stored in Transport for NSW's DRIVES system can only be accessed by paying a fee which is authorised under law. These requirements are set by the partner agency and not by Service NSW.

5.4.2.2 Making formal access requests under GIPA

Individuals can make a formal access request under the PPIP Act, HRIP Act or the *Government Information (Public Access) Act 2009* (GIPA Act), without first making an informal request. A formal application under the GIPA Act may be required if any of the following applies:

- the information relates to a third party
- there are significant public interest considerations that need to be considered
- you request a large volume of information, or
- it would take a significant amount of time for us to consider your request.

For requests for information under the GIPA Act, we will acknowledge the formal request within 5 days and generally provide a decision on your request within 20 working days.

No fee is required to request information under the PPIP or HRIP Acts, however GIPA applications will require an application fee of $30, and you will need to go through a proof of identity check if you are seeking personal information.

Information about making a formal request for information under the GIPA Act is available on the Service NSW website here.

5.4.2.3 How to make a formal request under the PPIP or HRIP Act

Individuals can make a formal request to access or amend personal information under the PPIP Act or health information under the HRIP Act by contacting the Privacy Officer. You should provide us with the following information:

- your name and contact details, including your postal address, telephone number and your email address
- indicate whether you are making the application under the PPIP Act (personal information) or HRIP Act (health information)
- explain what personal or health information you wish to access or amend
- explain how you want to receive the information or outcome of the amendment request; we usually do this through a secure transfer method.

You will need to go through a proof of identity check. Depending on the sensitivity and complexity of an access request, we may ask you to complete an Access to Personal Information Application Form which we will send to you.

5.4.2.4 Service NSW staff accessing their own personal information

Service NSW staff can access and, in many cases, amend their personal information contained in enterprise resources planning (ERP) systems and other systems provided to do your work. If you require access to or wish to amend your personal or health information beyond ERP systems, contact your HR Business Partner.

You have unlimited access to your personal information held by us through SAP and MyCareer. This includes your pay slips, leave balances, comments from your supervisor, timesheets, and other types of personal information.

Certain information is maintained at a local business unit level or 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. Please contact your line manager if you require access to this type of information.

5.4.3 Correction IPP8 and HPP8

Service NSW must, at your request, update, correct, delete, or amend your personal information where necessary.

In addition to the right to seek amendment of personal and health information above, Service NSW provides mechanisms for customers to correct their personal information as part of our customer service functions. We actively encourage and remind customers and employees 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 in their MyServiceNSW Account, 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 the relevant record is controlled by a partner agency and not by Service NSW, we may refer the request to the partner agency to correct your information. For example, in those instances where a partner agency has not provided Service NSW with access to their systems to amend information.

If we disagree 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 amendment, for processing such a request or for making an amendment.

5.5 Using personal and health information (IPPs and HPPs 9-10)

The 'use' principles govern how we may use the personal and health information that we hold. In this section we explain the reasonable steps we take to check information before use to ensure it is accurate and up to date. We also outline how we use your information after collection and explain the difference between 'primary' and 'related secondary' use.

5.5.1 Accurate use IPP9 and HPP9

Service NSW must ensure that your personal information is relevant, accurate, up to date, complete and not misleading before we use it.

Service NSW meets this requirement by having processes built into normal operating procedures to check the accuracy of your information before we use it.

For example, when individuals log in to a MyServiceNSW Account, they will be prompted to check and update personal details when using the Profile Connect feature. This ensures that we will be using the correct contact details for the transaction that is about to be performed. Likewise, when a customer visits one of our Service Centres, we'll ask to verify their personal information while processing a transaction.

If Service NSW collects personal and health from a partner agency when exercising functions on its behalf, we rely on the steps taken by the agency to ensure that the information is accurate before we use it.

If Service NSW receives information from a third party that customer details have changed, we will contact you to verify the information prior to amending it.

5.5.2 Limited use IPP10 and HPP10

Service NSW can only use your personal information for the purpose for which we collected it 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 your health or safety.

We will generally use personal and health information for the purpose for which it was collected. This is explained in the privacy collection notice that was provided to you at the time you received a particular service. This is known as the *primary purpose.*

For example, when a MyServiceNSW account is created, we use the information collected in the profile to pre-complete online forms, making it quicker to complete transactions or access services delivered by us or another NSW Government agency. This is one of the primary purposes for collecting information through your MyServiceNSW Account profile.

We may also use information for *directly related secondary* purposes such as auditing, reporting or program evaluation. 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 personal information to update a customer's contact information with other agencies.

Service NSW also collects, maintains and uses records of information about customer transactions and preferences, and other information, for internal administrative purposes. This includes:

- details of transactions between customers and Service NSW,
- customer preferences for how you transact and receive information from us and for our partner agencies
- other information about customers.

Service NSW staff should never use personal information beyond what the privacy collection notice states. If you are thinking of using personal information outside the primary or related secondary purpose, you must contact the Service NSW privacy team.

Service NSW may use some exemptions as it relates to the use of information we collect. Please see section 6 for more information.

5.6 Disclosing personal and health information (IPPs and HPPs 11-12)

5.6.1 Restricted disclosure IPP11 and HPP11

Service NSW can only disclose your information if we told you we would do so when we collected, or if you provide your consent. We may also disclose your information if it is for a directly related purpose and we reasonably assume that you would not object, or if disclosure is necessary to prevent a serious and imminent threat to your health or safety.

Service NSW makes our customers aware of routine disclosures that are likely to occur as part of accessing a service or performing a transaction with us. This is explained in the privacy collection notice that was provided at the time we deliver a transaction or service. There are some other circumstances where we may disclose information including if:

- the person has consented, or
- the information is not health information or other specific kinds of 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.

However, most routine disclosures we make are related to the primary purpose and will be explained in the privacy collection notice for that specific transaction.

5.6.1.1 Service NSW within the DCS cluster

Service NSW is an executive agency related to DCS; however, it is a distinct entity for privacy purposes. There is no special provision to disclose personal or health information to other DCS agencies. Any such disclosure must comply with privacy requirements.

Service NSW may disclose personal or health information to DCS in circumstances including:

- when seeking legal advice, where legal services are provided by DCS
- where disclosure is detailed in a privacy collection notice
- where we perform customer service functions for DCS
- to enable inquiries to be referred between the agencies concerned
- under a delegation to enable DCS to exercise employee functions.

Service NSW staff should never disclose personal information beyond what the privacy collection notice states. If there is a request to share personal information outside an agency listed in the collection notice you must contact the Service NSW Privacy team.

Service NSW may use some exemptions as it relates to the disclosure of information we collect. Please see section 6 for more information.

5.6.2 Safeguarded disclosure IPP12 and HPP14

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

Under privacy law, disclosing certain sensitive information (relating to ethnic, racial origin, political opinions, religious or philosophical beliefs, trade union memberships or sexual preference) is only allowed with your consent or if there is a serious and imminent threat to a person's life or health.

Service NSW does not routinely collect sensitive personal information of this nature when we exercise customer service functions. However, Service NSW provides customers with a voluntary option to provide their Aboriginal and Torres Strait Islander descent in certain cases. This information will:

- only be used for de-identified statistical purposes unless you consent otherwise
- only be disclosed to a partner agency with your consent where the information is requested, as part of a specific transaction between Service NSW and the partner agency
- not be disclosed for any purpose without your consent.

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

- you have provided consent
- it is necessary for a contract with (or in the interests of) the person concerned
- if we cannot obtain your consent but believe it would be to your benefit and that you would be likely to give your consent
- we have bound the recipient by contract to privacy obligations equivalent to the HPPs.

There are some circumstances where we may also disclose information in accordance with the information handling provisions set out in the Service Act.

5.7 Anonymity and unique identifiers (HPPs 12, 13, 15)

These principles relate to health information only, although we generally try and facilitate people to receive services from us anonymously when it is lawful, secure, and practical.

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

If you are making an informal enquiry or requesting general information, we will not ask you to identify yourself. However, we may not be able to provide a service or assistance to you without collecting your personal information. You can provide us with feedback on the online 'contact us' form without having to provide us with your personal or health information. However, if you wish to receive a response, we will collect your name and contact details.

Service NSW takes care not to inadvertently collect customers' health information. Where we do collect health information (for example, when applying for a Fertility Rebate) we do not give it a separate identifier, and do not include it in any health records linkage system.

Where health information has been gathered to case manage an injured Service NSW 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,

it is held against the investigation file and not given any separate identifier. There are no linkages to any health records systems.

5.8 Public registers

Some of our partner agencies publish information in a public register where required under law. However, Service NSW does not control any public register that contains personal or heath information.

6 Exemptions to IPPs and HPPs and Service Act protections

6.1 Exemptions

Exemptions allow public sector agencies to modify the application of the Information Protection Principles (IPPs) of the Health Privacy Principles (HPPs) in certain circumstances. Service NSW mainly relies on some exemptions to the PPIP Act and not the HRIP Act. Exemptions to the PPIP Act can be found in:

- the PPIP Act itself
- a regulation made by the responsible Minister
- a privacy code of practice, made by the Responsible Minister
- a Public Interest Direction, made by the Privacy Commissioner.

Staff should contact the Service NSW privacy team if you think you may need to use an exemption to modify the collection, use or disclosure of personal and health information.

6.1.1 Exemptions in the PPIP Act

Service NSW has a unique role in performing functions on behalf of NSW Government agencies. These functions come with some additional information handling provisions, which are detailed in the Service Act and modify the IPPs in certain ways.

Section 25 of the PPIP Act permits a modification of the IPPs where another Act (such as Service Act provisions referenced below) permits non-compliance. The provisions of the Service Act which permit the handling of personal information in particular ways, together with the most relevant exemptions that Service NSW may rely on under the PPIP Act, include:

Direct collection (IPP2)

- Section 14(4)(a) of the Service Act permits information to be disclosed to Service NSW by a Government agency for purposes of Service NSW delivering functions for that agency, or a related function.
- Section 27A of the PPIP Act permits Service NSW to collect personal information from another agency if reasonably necessary to enable inquiries to be referred between agencies or to manage correspondence from a Minister or member of Parliament or to enable the auditing of accounts of performance of an agency or agencies.

Open collection (IPP3)

- Section 15 of the Service Act permits Service NSW to refer individuals to another agency's privacy collection notice when we are exercising functions for that agency. The agency's privacy notice must contain the matters that individuals are required to be made aware of under IPP3.

Limited use (IPP10)

- Section 14(6) of the Service Act permits Service NSW to use information that has been disclosed to Service NSW under section 14 for purposes that it was disclosed.
- Section 23(4) of the PPIP Act permits Service NSW to use information other than for the purpose for which it was collected if it is for law enforcement purposes or for the protection of the public revenue.
- Section 27A of the PPIP Act permits Service NSW to use personal information if reasonably necessary to enable inquiries to be referred between agencies or to manage correspondence from a Minister or member of Parliament or to enable the auditing of accounts of performance of an agency or agencies.

Limited disclosure (IPP11 and 12)

- Section 14(1) of the Service Act permits Service NSW to disclose information to a partner agency where Service NSW has collected the information through the exercise of a customer service function to the partner agency. Service NSW can also disclose information to any person to whom the partner agency is authorised or required to disclose the information.
- Section 23 of the PPIP Act permits Service NSW to disclose information in order to investigate an offence where an offence may have been committed, for law enforcement purposes or for the protection of the public revenue.
- Section 27A of the PPIP Act permits Service NSW to disclose personal information if reasonably necessary to enable inquiries to be referred between agencies or to manage correspondence from a Minister or member of Parliament or to enable the auditing of accounts of performance of an agency or agencies.

6.1.2 Privacy code of practice

On 5 February 2026, a privacy code of practice was made by the Minister. The *Service NSW Fraud Management Privacy Code of Practice* modifies the collection, use and disclosure of personal information in certain circumstances.

The privacy code of practice is required for Service NSW to prevent, detect and investigate fraud related to the use of MyServiceNSW accounts and to support the function of Service NSW to detect fraudulent activity in grant, rebate and voucher programs. The following IPPs are modified through the privacy code of practice:

- Direct collection – IPP2
- Limited use – IPP10
- Limited disclosure – IPP11.

Section 4 of the code outlines the types of information that the Code applies to, including circumstances when the collection, use and disclosure of personal information may occur through the operation of the code. A copy of the Code is available on the Information and Privacy Commission website.

6.1.3 Public interest direction

Service NSW has a current Public Interest Disclosure (PID) in relation to life status checks for the NSW Digital Identity Pilot. This modifies the collection and disclosure principles to ensure the identities of deceased individuals are not being used to fraudulently create an NSW Digital Identity.

The PID enables ID Support NSW to conduct life status checks on behalf of Service NSW for the purpose of identity verification when a customer applies for an NSW Digital Identity. The Direction is in place until the relevant regulations under the *Identity Protection and Recovery Act 2025* (IPR Act) are made and Service NSW is approved as a 'fraud check user' under the IPR Act.

The PID commenced on 13 February 2026 and will last for 12 months. A copy is available on the IPC website here.

6.2 Information protected under the Service Act

Between 2020 and 2022 Service NSW supported the community during the COVID-19 pandemic by delivering services and initiatives that handled personal or health information.

Section 17B of the Service Act ensures that personal and health information collected by Service NSW under the public health orders cannot be used or disclosed except in very limited circumstances. The amendments prevent Service NSW from disclosing personal and health information collected under the public health orders for any use other than:

- the purpose for which it was collected
- contact tracing, including in another Australian jurisdiction
- to provide access to the person it is about
- or in limited circumstances to investigate a breach of the public health orders when it relates to the issue of a permit or a border declaration.

7 Your rights under privacy law

You have a right to complain 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 first to discuss any concerns with the staff member or business unit dealing with your information (if known).

You may make a complaint:

- by making a general privacy complaint to Service NSW
- by applying to Service NSW for an 'internal review' of the conduct you believe breaches an IPP and/or an HPP
- directly to the NSW Privacy Commissioner through their website, which may lead to a conciliated outcome.

7.1 Making general privacy complaints

General privacy complaints may include customers raising concerns (either in writing or verbally) through one of our Service NSW channels or may be made to the Privacy Officer or privacy team. Complaints could be about Service NSW's processes for handling their information, a privacy breach or other incident.

There are no external review rights to NCAT at the conclusion of a general privacy complaint.

If a customer is not satisfied with the outcome of their complaint, then they apply for a 'privacy internal review'. A customer has 6 months from first becoming aware of the relevant conduct to apply for an internal review. Service NSW may decline to deal with an application for internal review received after that period.

7.2 Requesting an internal review

Internal review is the process by which Service NSW manages formal, written privacy complaints about how we have dealt with personal information. You can request an internal review by contacting the Service NSW Privacy Officer, by phone on 13 77 88 or by email at privacy@service.nsw.gov.au .

An application for a privacy internal review doesn't need to use the words 'internal review' or specifically refer to the privacy legislation. However, to constitute an application for internal review, the written complaint must, on its face, reasonably convey to Service NSW that an application for internal review is sought.

The absence of any reference to privacy legislation, IPPs/HPPs or the concept of privacy may indicate to Service NSW that a complaint is an expression of grievance or request for action rather than an application for internal review. Where possible, Service NSW will attempt to clarify with customers their intentions in submitting a complaint to establish the customer's preferred pathway of a general complaint, internal privacy review or other outcome.

An internal review must be undertaken by the agency concerned. This means that, if you apply to Service NSW for an internal review of its conduct, Service NSW must undertake the review. Where an application for internal review relates to conduct by Service NSW exercising functions for a partner agency, Service NSW may conduct enquiries with the relevant partner agency in order to make findings and determine what action, if any, to take. Service NSW may determine the partner agency is the appropriate agency to conduct the internal review and will refer the application onto the partner agency.

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

- be in writing (either by post or by email)
- 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.

The IPC website provides a form for applying for internal review, as an optional resource. This can be downloaded from their website. Although we encourage you to use the form, it is not compulsory. You may submit any other relevant material along with your application.

7.2.1 What you can expect from us

Service NSW aims to acknowledge in writing our receipt of an internal review request with 5 working days. We are also required under the PPIP Act to:

- complete the internal review within 60 working days
- inform you of the outcome of the review within 14 working days of completing it.

If the review is not completed within these timeframes, you have the right to seek external review at the NSW Civil and Administrative Tribunal (NCAT). Normally, the internal review will be conducted by the Service NSW privacy team, 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.

We will determine whether Service NSW should manage the internal review alone or in consultation with a relevant partner agency. We will follow the Privacy Commissioner's internal review checklist and consider any relevant material submitted by you and/or the Privacy Commissioner.

As a result of the internal review, we may:

- take appropriate remedial action
- make a formal apology to you
- implement administrative measures to prevent the conduct occurring again
- undertake that the conduct will not occur again, or
- take no further action on the matter.

When we inform you of the outcome of the review we will include:

- the findings of the review
- the reasons for those findings
- the action Service NSW 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.

7.2.2 Role of the NSW Privacy Commissioner

Under the PPIP Act, Service NSW must inform the Privacy Commissioner:

- that we have received an application for an internal review
- of regular progress reports of the investigation
- on the outcome of the investigation
- of any proposed actions taken by us in response to the internal review.

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. Any submissions made by the Privacy Commissioner to us will be taken into consideration when making our decisions.

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

If you are not satisfied with the outcome of an internal review, you may apply to NCAT for an external review. 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 personal information
- provide an apology, or
- take steps to remedy loss or damage.

NCAT may also make an order requiring Service NSW to pay damages if you have suffered loss or damage because of our handling of your information.

8 Legislation and policies relating to personal and health information

8.1 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 2017*
- Codes of Practice, Directions and Statutory Guidelines made under the PPIP and HRIP Acts

8.2 Other relevant legislation

- *Crimes Act 1900 (NSW)*
- *Data Sharing (Government Sector) Act 2015 (NSW)*
- *Government Information (Public Access) Act 2009 (NSW) (GIPA Act)*
- *State Records Act 1998 (NSW)*
- *Workplace Surveillance Act 2005 (NSW)*
- *Surveillance Devices Act 2007 (NSW)*
- *Service NSW (One-stop Access to Government Services) Act 2013* (NSW)
- *Public Interest Disclosures Act 2022 (PID Act)*

8.3 Key DCS and Service NSW policies

The Service NSW privacy team has developed a range of guidance material to help staff understand how privacy operates in Service NSW, and how staff can protect the information Service NSW handles.

Service NSW privacy policies and guidance material can be accessed via the internal Service NSW intranet site. There are a range of other DCS policies and procedures that are related to the handling of personal information that staff can access via the DCS Intranet site.

Key policies related to the management of personal or health information include:

8.3.1 DCS Policies

- Records Management Policy
- Information Security Policy, including:
    - IT Security Policy
    - IT Acceptable Use Policy
    - IT Security Standards
    - Cloud Security Policy

- Code of Ethics and Conduct

8.3.2 Service NSW Policies and Standards

- Data Breach Policy
- Data Breach Response Plan
- Privacy Management Plan
- Privacy Management Framework
- Service NSW Complaints Policy
- Risk Management Framework
- Workplace Surveillance Policy
- Data Sharing Framework
- Retention and Disposal of Customer Data Policy
- Retention and Disposal Standard
- AI Acceptable Usage Standard
- Service NSW Cyber Security Standards

9 Appendices

9.1 Appendix A: Key Definitions

Head of agency

The Secretary of DCS is the Head of Agency for Service NSW.

Health Information

Health information is a is a 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 provider
- information or an opinion about a health service already provided to a person e.g. attendance at a medical appointment
- information or an opinion about a health service that is going to be provided to a person.

Health information principles

The 15 Health Privacy Principles (HPPs) are the key to the 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.

You can find the most up-to-date factsheet on the HPPs at https://www.ipc.nsw.gov.au/health-privacy-principles-hpps-explained-members-public

Information privacy principles

The 12 Information Protection Principles (IPPs) are the key to the 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.

You can find the most up-to-date factsheet at https://www.ipc.nsw.gov.au/information-protection-principles-public.

Mandatory Notification of Data Breach Scheme (MNDB Scheme)

A scheme that requires public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information in circumstances likely to result in serious harm.

Partner agency

A NSW Government agency, NSW local government entity, Commonwealth agency, agency of anther state or territory government or non-government entity that Service NSW exercises functions for under delegation or by agreement.

Personal information

Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information can include a person's name, address, financial information, and other details including photographs, images, video, or audio footage.

The definition of personal information does not include information or opinion about a person's suitability for employment as a public sector official or information about a person:

- that has been dead for more than 30 years
- that is contained in a publicly available publication.

Sensitive information

Information referred to in section 19(1) of the PPIP Act. A specified type of 'personal information', which comprises information relating to a person's race, ethnicity, religion, sexuality, political or philosophical beliefs or membership of a trade union. The PPIP Act and HRIP Act provides stricter safeguards on managing information of this nature.

Service partnership agreement

The agreement Service NSW enters into with partner agencies and organisations, which stipulates the terms, conditions, requirements, specifications, and responsibilities regarding the transactions Service NSW completes on the agency's behalf.

Staff

All Service NSW employees, Senior Executives, contractors, and service providers who collect, store, use, and disclose personal and health information as part of their daily duties.

9.2 Appendix B: Key contacts

Service NSW privacy officer

Phone:	13 77 88
Email:	privacy@service.nsw.gov.au
Website:	www.service.nsw.gov.au/privacy
Mail:	Service NSW privacy officer Enterprise Risk and Enablement GPO Box 7057 Sydney NSW 2001
Office:	McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

The Information and Privacy Commission NSW

Phone:	1800 472 679
Email:	ipcinfo@ipc.nsw.gov.au
Website:	www.ipc.nsw.gov.au
Mail:	Information and Privacy Commission NSW GPO Box 7011 Sydney NSW 2001
Office:	Level 15 McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

The NSW Civil and Administrative Tribunal

Phone:	1300 006 228 and select Option 3 for all Administrative and Equal Opportunity Division enquiries
Email:	aeod@ncat.nsw.gov.au
Website:	www.ncat.nsw.gov.au
Mail:	NSW Civil & Administrative Tribunal Administrative and Equal Opportunity Divisions PO Box K1026 Haymarket NSW 1240 | DX 11539 Sydney Downtown
Office:	John Maddison Tower, 86-90 Goulburn Street, Sydney

9.3 Appendix C: Partner Agencies

Building Commission NSW
Civil And Administrative Tribunal Of New South Wales
Combat Sports Authority
Cyber Security NSW
Department Of Climate Change, Energy, The Environment And Water
Department Of Communities And Justice
Department Of Customer Service
Department Of Education
Department Of Planning, Housing And Infrastructure
Department Of Primary Industries And Regional Development
Environment Protection Authority
Fire And Rescue NSW
Government Technology Platforms (GTP)
Health Administration Corporation
Health Professional Councils Authority (HPCA)
Hunter Water Corporation
Insurance And Care NSW (icare)
Investment NSW
Liquor And Gaming NSW (L&G)
Long Service Corporation
Ministry Of Health (MoH)
Multicultural NSW
National Heavy Vehicle Regulator
National Roads And Motorists' Association Limited (NRMA)
Nepean Blue Mountains LHD
New South Wales Treasury Corporation
NSW Crown Lands
NSW Environmental Protection Authority (EPA)
NSW Fair Trading
NSW National Parks And Wildlife Service
NSW Police Force
NSW Reconstruction Authority
NSW Reconstruction Authority Staff Agency

NSW Registry Of Births Deaths And Marriages
NSW Telco Authority
NSW Trains
NSW Treasury
NSW Trustee And Guardian
Office Of Local Government
Office Of Sport
Office Of The Ageing And Disability Commissioner
Office Of The Children's Guardian
Personal Injury Commission
Premiers Department
Queensland Government- Australian Coordinating Registry Department Of Justice And Attorney-General
Revenue NSW
Safework NSW
St John Ambulance Australia (N.S.W.)
State Insurance Regulatory Authority
Subsidence Advisory NSW
Tollaust Pty. Limited
Transport For NSW
Volunteer Marine Rescue NSW
Western Sydney Local Health District

Document Approval

Name and Position	Date
Amie Grierson, Director Privacy and Fraud	29 April 2026