Privacy Management Plan

March 2021

Policy Statement

This Privacy Management Plan (PMP) meets the requirement for such a Plan under section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) by demonstrating to members of the public how the Department of Customer Service (DCS) meets its privacy obligations under that Act and the *Health Records and Information Privacy Act 2002* (HRIP Act) and upholds and respects the privacy of our customers, employees and others about whom we hold personal information. It also acts as a reference for employees of DCS, to explain how we comply with the requirements of the PPIP and HRIP Acts, and to prompt DCS employees, contractors and service providers to seek further advice where unsure about applicable privacy requirements.

This PMP sets out the privacy obligations of DCS, explains which exemptions DCS commonly relies on and sets out the process for undertaking privacy internal reviews. DCS is part of a NSW Government 'cluster', 'the Customer Service Cluster', and therefore this PMP covers a number of cluster entities, in addition to DCS itself. The scope of this PMP is explained in the introduction below.

DCS commits itself to operating in accordance with this PMP and regularly reviews its performance against this PMP. DCS will review this PMP quarterly at a minimum, and update it as required.

Approved by	
Name: Emma Hogan	
Title: Secretary	**Date:** March 2021

This plan was last reviewed in March 2021.

Privacy Management Plan

Contents

Definitions

Business Unit	A work unit performing a discrete business function within a government agency. Multiple business units make up divisions.
Cluster	NSW Government departments, agencies and organisations are arranged into nine groups which reflect broadly the policy areas of Government. These nine groups are consolidated NSW Government entities called 'clusters.' The Customer Service cluster is one of these clusters.
Cluster entities	DCS, a central department in the NSW Government, has over 30 agencies, divisions, and business units. Each of these entities are referred to as 'cluster entities'.
DCS or Department of Customer Service	Refers to the Department of Customer Service cluster.
Health information	As defined in section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act) health information 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 service 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 • a health service a person has requested • some genetic information.
Health Privacy Principles (HPPs)	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. The most up-to-date factsheet may be found at https://www.ipc.nsw.gov.au/health-privacy-principles-hpps-explained-members-public
Information Privacy Principles (IPPs)	The 12 Information Protection Principles (IPPs) are the 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. The most up-to-date factsheet may be found at https://www.ipc.nsw.gov.au/information-protection-principles-public

Public sector agency	A 'public sector agency', as defined in section 3 of the PPIP Act. This includes the following: (a) a Public Service agency (b) a statutory body representing the Crown (d) a person or body in relation to whom, or to whose functions, an account is kept of administration or working expenses, if the account— (i) is part of the accounts prepared under the Public Finance and Audit Act 1983, or (ii) is required by or under any Act to be audited by the Auditor-General, or (iii) is an account with respect to which the Auditor-General has powers under any law, or (iv) is an account with respect to which the Auditor-General may exercise powers under a law relating to the audit of accounts if requested to do so by a Minister of the Crown.
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.
Separate public sector agency	An entity that is not a part of DCS for the purposes of the PPIP Act.

PART A - Introduction

Introduction to the Department of Customer Service and its privacy context

The Department of Customer Service (DCS) is a central agency in the NSW Government. We are a service provider and regulator focused on improving customer experience across government agencies. We do this by improving laws, designing and implementing customer-centric services and initiatives informed by data analytics and behavioural insights, and making it easier to do business in NSW. We collect, hold, use and disclose personal and health information for the purpose of carrying out these functions and activities.

Our lead cluster Minister is the Minister for Customer Service, who is accompanied by the Minister for Better Regulation and Innovation and the Minister for Finance and Small Business.

DCS and the Department of Customer Service cluster

DCS is a public sector agency within a 'cluster' model. Government cluster models are an administrative construct and are not legally defined. The Customer Service cluster comprises several other agencies. Under the 'cluster' model, DCS provides employees to several other agencies in the cluster to allow them to carry out their functions. For example, the employees who perform the functions of the Long Service Corporation, a part of the Customer Service cluster, are employed by DCS. This PMP sets out the privacy obligations of DCS including cluster entities whose employees are employed by DCS, explains which exemptions we commonly rely on and sets out the process for undertaking internal reviews. References to DCS in this PMP generally include references to cluster entities unless the context indicates that they do not.

Please see 'Appendix 4: Detailed List of DCS Cluster' (Page 41) for further information on individual agencies, offices, entities and business units within the DCS cluster.

Information sharing and use within DCS

A strong focus of DCS is on the provision of customer services and better regulation. The sharing of information between divisions and with other agencies can be vital to achieve these goals. We take privacy seriously and manage your personal and health information.

We collect and hold personal or health information that allows us to carry out our daily operations. This may include information required to process workers compensation claims and disputes, consumer and trading complaints, land tax calculations or requests under right to information laws.

The information collected for any DCS function may be used by DCS for a primary or directly related secondary purpose as allowed under legislation. A primary purpose is the clear purpose for which we collect the information from you, for example for a licence application. Directly related secondary purposes might include investigations, improvements in customer service, policy and programs, or responding to ministerial enquiries. We take guidance from the DCS Privacy Management Framework to ensure that the disclosure of information by one DCS division to another adheres to the information protection and health privacy principles.

Applicable privacy laws

As a "public sector agency", the handling of personal and health information by DCS is regulated by the NSW privacy laws:

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

The PPIP Act regulates the handling of "personal information" by public sector agencies. "Personal information" is any information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. The PPIP Act requires agencies to comply with 12 Information Protection Principles (IPPs). The IPPs cover the full "life cycle" of information as it moves through an agency, 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.

The HRIP Act regulates the handling of "health information" by public sector agencies. "Health information" is like a special type of personal information. It includes information or an opinion about the physical or mental health or disability of an individual, a health service provided to an individual or other personal information collected to provide a health service. The HRIP Act requires entities to comply with 15 Health Privacy Principles (HPPs). The HPPs are similar to the IPPs but are not identical. 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 exceptions and exemptions to many of the privacy principles and certain types of information are excluded from the definitions of "personal information" and "health information". These can be found in the two Acts themselves, and in Regulations, Privacy Codes and Public Interest Directions.

Part 2, Division 3 of the PPIP Act contains exemptions that may allow DCS or entities to whom this PMP applies to not comply with the IPPs in certain situations.

Some examples include:

- DCS is not required to comply with IPPs 2, 3, 6, 7, 8, 10, 11 or 12 if lawfully authorised or required not to comply, or compliance is otherwise permitted or is necessarily implied or reasonably contemplated under an Act or law.
- DCS is not required to comply with IPPs with respect to collection if the information concerned is collected for law enforcement purposes. However, this subsection does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.
- DCS is not required to comply with IPP 2 (direct collection) if the information concerned is collected in relation to court or tribunal proceedings.
- DCS is not required to comply with IPPs with respect to collection, use or disclosure of personal information if the collection, use or disclosure of the information is reasonably necessary:
    - to enable enquiries to be referred between the entities concerned, for example, for the use of corporate services of another agency. However, prior to doing so the agency will either deidentify all personal information before seeking advice from another agency or will obtain prior consent from the individual who the information is about before disclosure or may rely on any available exemptions, or
    - to enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies (or a program administered by an agency or group of entities, or
    - to allow any of the entities concerned to deal with, or respond to, correspondence from a Minister or member of Parliament.

Please see “Sometimes the IPPs and HPPs do not apply” in Part D, and Appendix 2 for other general exemptions which DCS may rely upon.

Public interest directions can modify the IPPs for any NSW public sector agency, and are available on the Information and Privacy Commission (IPC) website: https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/public-interest-directions. Currently, there are no directions in operation that are likely to affect how DCS or its entities manage personal information.

Some agencies or divisions will also have a Privacy Code of Practice, which are available on the IPC website: https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/privacy-codes-practice. This is a document approved by the NSW Privacy Commissioner that provides for specific exemptions for some agencies or divisions from the IPPs in order to carry out their functions. Relevant codes of practice that may affect how DCS or the agencies to whom this PMP applies manage personal information are:

- Privacy Code of Practice for the NSW Fair Trading, and
- Privacy Code of Practice (General) 2003 (Part 7 dealing with Registry of Births, Deaths and Marriages).

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:

- customers
- employees
- persons conducting a business or undertaking
- insurers
- regulators
- 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

Responsibilities of all DCS employees, contractors and service providers

All employees, agents and contractors of DCS are required to comply with the privacy principles set out in the PPIP Act and HRIP Act. Both Acts contain criminal offence provisions applicable to employees, agents and contractors who use or disclose personal information or health information other than in accordance with their lawful functions.

Employees who are suspected of conduct that would breach the privacy principles or the criminal provisions may be disciplined for a breach of the DCS Code of Ethics and 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 DCS (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*.

Notification of Data Breach

DCS, upon becoming aware of a data breach which involves personal or health information which may result in serious harm or having a reasonable suspicion that a data breach has occurred which is likely to result in serious harm, has a practice of voluntarily notifying the IPC and conducting an assessment to determine the circumstances of the breach or suspected breach, and of notifying customers who may be at risk of suffering serious harm.

Privacy Officer for DCS

Governance, Risk and Performance, Corporate Services

Mail: GPO Box 7057, Sydney NSW 2001
Phone: 13 77 88
Email: privacy@customerservice.nsw.gov.au

Governance, Risk and Performance

The Executive Director for Governance, Risk and Performance (GRP) in the Corporate Services division is the DCS Privacy Officer, responsible for providing governance services to a portfolio of divisions. The DCS Privacy Officer leads a dedicated Privacy Team which has responsibility for managing DCS's privacy management functions. These functions include providing guidance to DCS employees, contractors, or service providers on their privacy obligations, and how to manage personal and health information in their day-to-day work.

Responsibilities of the DCS Privacy Officer

The DCS Privacy Officer is responsible to:

- ensure the PMP remains up to date
- publish the PMP
- inform employees and contractors of any changes to the Plan

- make a range of guidance material available to DCS employees, contractors, and service providers to help them understand their privacy obligations, and how to manage personal and health information in their everyday work
- provide privacy expertise to assist the adoption of a privacy-by-design approach to the development of new products and services, and to the existing products and services as they evolve
- recommend controls to help manage privacy risks, and providing privacy expertise to assist their implementation
- respond to privacy incidents
- handle privacy complaints
- maintain reporting on privacy incidents, complaints, and other relevant metrics
- provide privacy training and awareness activities to DCS employees, contractors, and service providers, and
- be available to answer any questions DCS employees may have about their privacy obligations.

In carrying out these responsibilities, the DCS Privacy Officer may work with the privacy officers across the cluster, where appropriate.

The Privacy Officer, in accordance with clause 6 of the *Annual Reports (Departments) Regulation 2015,* is to ensure that the DCS 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 PMP:

- if DCS 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 DCS, or
- at the conclusion of the 2020-21 reporting year.

The Secretary of DCS, 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 and the DCS intranet 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 DCS Privacy Officer is also responsible for answering questions from members of the public about the content or operation of the PMP and handling any privacy complaints or non-routine requests for access to or correction of personal or health information.

PART B: DCS and its agencies, entities, and business units

DCS is one of nine clusters across the NSW Government. Clusters have no legal effect for privacy purposes. DCS must comply with the applicable privacy principles. Where we use personal or health information internally, this will constitute a "use" for privacy purposes. Where we provide information to another person or body, including another separate public sector agency within the Customer Service cluster, this will constitute a "disclosure" for privacy purposes.

DCS employees should be aware that there is no special provision for giving personal or health information to other agencies within the Customer Service cluster. Care should be taken to ensure that any such disclosure complies with applicable privacy requirements. If you are not sure, check with the DCS Privacy Officer.

We may disclose personal or health information to a Customer Service cluster entity in circumstances including:

- to enable inquiries to be referred between the agencies concerned, or
- under a delegation to enable DCS to exercise employee functions, or
- where the disclosure is reasonably necessary for law enforcement purposes, including the investigation of suspected fraud.

The DCS cluster houses individual agencies, offices, entities and business units that carry out various functions. Further details are provided in Appendix 4.

Are all DCS cluster entities covered by the DCS PMP?

The PPIP Act requires that each public sector agency must prepare and implement a PMP. Any entity which is a part of DCS is covered by the DCS PMP.

Separate public sector agencies are not a part of DCS for the purposes of the PPIP Act. However, clause 6 of the *Privacy and Personal Information Protection Regulation 2019* (PPIP Regulation) modifies the requirement for a public sector agency to have their own PMP if their staff are a part of the staff of DCS and the DCS PMP states the plan will extend to that agency. DCS Privacy may not perform privacy internal reviews for these separate public sector agencies but will work with the appropriate privacy officers across these public sector agencies.

Please see Appendix 4 for a list of the entities which are covered by the DCS PMP. The DCS PMP does not extend to the entities listed in Table A.

Table A – List of entities that are not covered by the DCS PMP

Name of the entity	Does the DCS PMP apply?
Revenue NSW	No
Hardship Review Board	No
Independent Pricing and Regulatory Tribunal (IPART)	No
Independent Liquor and Gaming Authority (ILGA)	No
Information and Privacy Commission (IPC)	No
NSW Architects Registration Board	No
Office of the Greyhound Welfare and Integrity Commission (GWIC)	No
Office of the Independent Review Officer (IRO)	No
Personal Injury Commission (PIC)	No

Note: PIC replaced the Workers Compensation Commission on 1 March 2021	
Service NSW	No
State Insurance Regulatory Authority (SIRA)	No

Internal reviews: Who will conduct the review?

Under the PPIP Act, internal reviews must be undertaken “by the public sector agency concerned”.

A person who is aggrieved by the conduct of any entity that is a separate “public sector agency”, is entitled to a review of that conduct. The review must be undertaken by the agency concerned and be dealt with by an individual within that agency. The internal review must be conducted by an employee or officer of that agency, as far as is practicable.

Although the PPIP Regulation allows the DCS PMP to extend to some entities which are separate “public sector agencies”, these entities are still separate “public sector agencies” for the purposes of the PPIP Act.

This means the DCS Privacy Officer, unless there is an existing contactable entity Privacy Officer, will conduct internal reviews which concern the conduct of DCS. Where a request for an internal review concerns the conduct of a separate “public sector agency” as defined under the PPIP Act, an employee or officer of that agency will conduct the internal review, as far as is practicable.

Please see Appendix 5 for a list of Privacy Officers who will, as far as practicable, conduct the internal reviews for the separate public sector agencies in the DCS cluster.

PART C: Types of personal and health information we hold

Due to our diverse nature, the type of personal and health information held is also diverse. There are two main categories of personal and health information that we hold or have access to:

- personal and health information about members of the public and stakeholders ('customer records'), and
- personal and health information about our employees, contractors, and service providers ('employee and contractor records').

Customer records

To exercise our various functions and activities, we hold personal or health information obtained through the NSW tax system, fair trading or home building disputes, licence and certificate applications, and so on. We may hold the following personal and health information, depending on the specific needs of the entity:

• Name and contact details	• Date of birth	• Signatures
• Wages/Income details	• Correspondence	• Complaints
• Tax file numbers	• Payroll tax	• Interpreter use
• Home address	• Employment details	• Financial and bank accounts
• Job specifications and status	• Insurance information	• Land title information
• Bankruptcy information	• Investigations	• Insurance and claims history
• Medical certificates and injuries	• Criminal records	• Compliance history
• Educational information (e.g. for licences)	• Records relating to births, deaths and marriages	• Details of workplace injuries and notifications

The above list is not exhaustive, and we may also hold other personal or health information provided for a range of specific functions of our agencies across the DCS cluster. We may collect information electronically, via email or over the phone.

Employee and contractor records

The types of personal and health information we hold about our employees and contractors includes:

- identity, demographic and contact data such as name, address, telephone numbers and email address, date of birth, gender, and signature
- education records
- payroll, attendance and leave records
- bank account and financial records
- performance management and evaluation records
- referee reports
- redundancy and termination decisions
- workers' compensation records
- work health and safety records
- medical assessments, records, and certificates, and
- records of gender, ethnicity, and disability of employees for equal employment opportunity reporting purposes.

People and Culture

An employee of DCS may access their own personnel file without cost. Apart from the employee the file relates to, others who may have authorised access to personnel files include People and Culture employees, nominated GovConnect employees and any other authorised delegates.

Where necessary, People and Culture may be required to arrange a health assessment for an employee or contractor. In doing so, People and Culture may be required to disclosure certain personal or health information to the organisation conducting the medical assessment who act as an agent for DCS. Similarly, People and Culture may be required to disclose certain personal or health information to insurers in order to process an employee or contractor's claim.

Managers

To carry out their role, DCS employees in managerial roles may hold and have access to the personal information of employees who report to them. This information is held in SAP and may be held in Office 365 applications, including for example performance management and evaluation records.

Self-service function

DCS employees and contractors have access to some soft copy records contained in DCS's enterprise business software used for managing employee and contractor information. This means employees have direct access to view and edit information, including applying for leave, viewing pay details, updating bank details, address, and email.

GovConnect

We maintain most employee and contractor personnel files centrally. Case management of injured employees and investigations of workplace incidents are dealt with by the DCS business unit known as People and Culture. Day to day operations of most employees, 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. Certain employee details are disclosed to GovConnect for them to provide the payroll service.

The information held by People and Culture and GovConnect can include salary and payroll tax information, medical information, grievances and investigations, and employment history including disciplinary actions.

Some information is maintained at a local division or business unit level, or is accessed by divisions or business units, for management purposes. This includes storing and using employees' personal and health information on internal databases for management purposes, case review and training.

Human resource practices and procedures are governed by several pieces of legislation as well as various policies, procedures, and guidelines for the public service:

- *Government Sector Employment Act 2013* and associated Rules and Regulations
- *Industrial Relations Act 1996* and associated Regulations
- *Work Health and Safety Act 2011* and associated Regulations
- *Workers Compensation Act 1987* and associated Regulations
- Any other relevant guidelines, policies or procedures from the NSW Ombudsman, the Public Service Commission, the Department of Premier and Cabinet, or other central oversight agencies.

The collection, use, storage, and disclosure of employee information is addressed in Part D below.

PART D: How we manage personal and health information

This section explains how we handle personal and health information. The PPIP Act and HRIP Act outline principles for managing personal and health information. These principles apply to all NSW government agencies and regulate the collection, storage, use and disclosure of personal and health information.

Addressing the principles

There are 12 IPPs set out in Part 2, Division 1 of the PPIP Act and 15 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.

1. Collection of personal information must only be for a lawful purpose (IPP 1 and HPP 1)

1.1. The principle in brief

We will only collect personal and health information if:

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

1.2. How we apply this principle

We won't collect personal information unless we need it for one of our functions. Some of our divisions and business units may also liaise with external stakeholders in order to fulfil our functions under legislation and we will seek to access the personal and health information collected by those stakeholders if it is reasonably necessary for those functions. For example, we may obtain personal information from a training provider when verifying qualifications for processing licence or certificate applications or may obtain health information from an insurer for processing a worker's compensation claim. Similarly, some divisions within DCS may obtain personal or health information from other divisions within the agency where it is necessary to carry out our functions or for directly related secondary purposes authorised by law. An example of a directly related secondary purpose could include an investigation of a real estate licensee, using information collected for the issue of the licence or using information collected during a licence application process to send licence renewal notices. We may also use health information to lessen or prevent a serious threat to public health or safety, manage provision of health services, provide training, research purposes and for law enforcement purposes, including suspected unlawful activity and unsatisfactory professional conduct.

A substantial amount of personal and health information is collected from our employees 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 employee within a division, when it is lawfully authorised and necessary for employee 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.

2. Personal information must only be collected directly from the person the information is about or someone authorised by that person (IPP 2 and HPP 3)

2.1. The principle in brief

The various divisions within DCS collect a range of information. We collect personal information direct from the person unless they have authorised otherwise. We collect health information directly from the person unless it is unreasonable or impracticable to do so. We will obtain some information from others where we are lawfully authorised to do this.

2.2. How we apply this principle

We collect your personal and health information directly from you unless you have authorised us to do otherwise. However, there are circumstances when information may have been gathered from other sources, including other government agencies, where we are lawfully authorised to do this under a legislative provision or a Privacy Code of Practice.

Different parts of DCS are required to gather certain personal information to carry out our functions. For example, health information relating to workers compensation and motor accident compensation fund claims may be obtained from others, such as insurers and scheme agents. Likewise, complaints or disputes lodged with Fair Trading require one party to the dispute to provide the name and contact details of the opposing party so that Fair Trading can mediate or investigate the matter. Human resources personnel may need to liaise with an injured employee's doctor. We will take what steps are necessary to ensure that collection of such information is done lawfully, such as getting consent from an employee to contact their treating doctor.

We only obtain personal or health information from another source where it is lawfully authorised. Lawful authorisation may be provided by a specific legislative provision or through a legal instrument such as a Privacy Code of Practice. Provisions authorising collection from another source generally set out the limited circumstances in which the information can be gathered. For example, section 20 of the Fair Trading Act 1987 allows a person appointed as an investigator under that Act to serve a notice on any person requiring the production of information, documents or evidence where it is relevant to a possible breach of that Act. In Safework NSW we may need to collect health information for the purpose of investigating workplace incidents and illnesses. SafeWork NSW inspectors will comply with this principle by following the procedure set out in the SafeWork NSW procedure: Obtaining Health Information (medical records and reports).

3. Notification when collecting personal information (IPP 3 and HPP 4)

3.1. The principle in brief

When collecting personal and health information from you, we will take reasonable steps to tell you:

- who we are and how to contact us
- what the information will be used for
- what other organisations (if any) we intend will receive this type of information from us
- whether the collection is authorised by law or is voluntary
- what the consequences will be if you do not provide the information to us
- how you can access and correct your information held by us, and
- the name and address of the agency that is collecting the information and the agency that is to hold the information.

3.2. How we apply this principle

When collecting health information about you from someone else, we take reasonable steps to tell you these things unless this would pose a serious health threat, or otherwise in accordance with NSW Privacy Commissioner guidelines.

We endeavour to ensure all forms across DCS that collect personal or health information, such as application forms, etc, include clear privacy statements with the above information. We will continue to review and refine the various forms across DCS to ensure they meet this requirement.

Sometimes information may be collected by DCS over the phone or face to face. Employees are trained to ensure they understand the privacy principles. Where appropriate, phone scripts will include a privacy statement to ensure employees provide information on the above points to you when they are collecting personal or health information from you.

4. How we collect personal information – the method and content (IPP 4 and HPP 2)

4.1. The principle in brief

When we collect personal and health information from you, we will take reasonable steps to ensure the information we collect is:

- relevant, accurate, up-to-date, and complete, and
- not intrusive or excessive.

4.2. How we apply this principle

We will take reasonable steps to ensure that when we design forms, communicate with members of the public and employees (face to face, over the phone and in writing), or otherwise collect information from you, we do not seek personal or health information that is intrusive or excessive. We will ensure that the personal and health information we do collect is relevant, accurate, up-to-date, and complete. We may do this by checking the information directly with you, or by cross referencing the information with other sources, such as the Australian Securities and Investment Commission's register of companies and business names, or with the Australian Tax Office's register of ABN numbers. We will also make sure that, if you request it, you can see what information we hold about you and we will correct it as necessary.

We design forms to ensure that only information required to carry out our functions is requested or required from you. We will ensure these privacy principles are built into our contact centres' policies and practices through employee training and through phone scripts.

5. How we store and secure personal and health information (IPP 5 and HPP 5)

5.1. The principle in brief

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

5.2. How we apply this principle

We consider the security of information to be an important issue and have systems in place to ensure that only authorised people can access information. All employees, including contractors, are required to

comply with the DCS Code of Ethics and Conduct. In addition, the PPIP Act carries several provisions for prosecuting individuals for unlawful disclosure of personal information, and s 308H of the *Crimes Act 1900* makes it an offence to access computerised records for a purpose other than official duties. Unlawful access to information by our employees, agents or contractors will result in disciplinary action, and in some serious cases, in criminal prosecution.

We use technical, physical, and administrative actions, as well as assessment by independent audit, as security measures to ensure personal and health information is stored securely. Some examples of retention and security measures that we have in place include:

- All our databases that are administered by DCS's ICT area that hold personal or health information are restricted by password or other security measures to ensure that only people with a reason have access to that information. Some business units may have local databases using Microsoft Access or Excel that are only accessible to the employees who work in that area and therefore only relevant employees have access to the information.
- For DCS networks, a minimum password standard is applied, including that employees change passwords on a quarterly basis and be suitably complex.
- Multi-factor authentication as an additional security measure to validate identity when accessing online applications from outside of DCS networks.
- Secure destruction bins or paper shredders are provided for disposal of confidential paper records where necessary. System access warnings are given when access attempts to confidential systems are made.
- Security audits are conducted of electronic systems access and databases, and of access and exit from DCS premises.
- Limiting access to sensitive information to only those who require access to perform lawful functions.

Access to electronic records keeping systems is restricted to the appropriate team, business unit or division, depending on the content, so that only those who need to access your data in order to carry out their functions can do so. Generally, once the 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.

Some areas maintain paper records, and these are stored either in a secure storage system onsite, such as lockable compactus or filing cabinet, or are sent to the Government Records Repository (GRR). GRR stores information in accordance with the provisions of the *State Records Act 1998* and standards issued by State Archives NSW.

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 room where personal or health information is stored may be restricted to authorised personnel.

6. Transparency (IPP 6 and HPP 6)

6.1. The principle in brief

Once we have confirmed your identity, we will take reasonable steps to let you find out:

- whether we are likely to hold your personal or health information
- the nature of the information we hold
- the purposes for which we used your personal or health information, and
- how you can access your information.

6.2. 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 collection notification (outlined in point 3 above), which is specific, and given at the time of collecting new personal or health information. Any information that is not required to be kept as a State record, and that is no longer needed to be kept, will be disposed of securely.

The PMP for DCS and, where applicable, PMPs for separate public sector agencies within DCS, will be available through the DCS website, any appropriate division's website and by request. These will set out the major categories of personal and health information that is held by the relevant division, explain the privacy obligations, and explain the process for accessing and/or amending any of the personal and health information we hold about you.

7. Access to information we hold (IPP 7 and HPP 7)

7.1. The principle in brief

You can make enquiries at any time to find out if we hold personal or health information about you. Once we have confirmed your identity, you may access your personal and health 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 in line with our commitment to be open and transparent.

7.2. How we apply this principle

If you want a copy of your own personal or health information held by DCS, we will usually be able to provide it to you, free of charge, directly from the appropriate business unit.

Please see Appendix 5 of this PMP for details to request access to information held by separate public sector agencies in the DCS cluster.

If you are having difficulties accessing your personal or health information, or you wish to make a formal application for information, you can contact the DCS Privacy Officer.

8. Correction of information we hold (IPP 8 and HPP 8)

8.1. The principle in brief

Once we have confirmed your identity, you may update or amend your personal or health information held by us to ensure it is accurate, relevant, up-to-date, complete, and not misleading.

8.2. How we apply this principle

DCS may wish to verify the accuracy of any information you request be amended, such as confirming qualifications with a training provider or information about a bankruptcy with the Bankruptcy Trustee.

In general, any proposed corrections to your personal or health information should be provided in writing so we can verify your identity and keep a record of the correction. You can send any requests for correction of your information directly to the appropriate agency or to privacy@customerservice.nsw.gov.au.

If we do not agree to the correction or amendment, the reason for the refusal will be provided in writing to person the information refers to and the applicant requesting the amendment. The request to amend, and any reason for a refusal to amend, must be saved adjacent to the information it refers to for the life of the information record.

If we correct or amend a record, we will endeavour to contact any affected parties within 30 days of the change, and only where the notification is necessary to adhere to the principles outlined in this PMP.

A disputed record may be a professional opinion that is challenged. However, the record of the professional opinion must be maintained regardless of the individual's request to vary that opinion.

9. Accuracy of information (IPP 9 and HPP 9)

9.1. The principle in brief

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

9.2. How we apply this principle

We ensure the accuracy of the information by collecting it directly from you wherever practicable, or otherwise in accordance with legislation (as set out in point 2 above).

We take such steps as are reasonable in the circumstances to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading. This may be achieved through the requirement of supporting documentation or by confirming the information with an outside agency. For example, an individual's previous involvement in a company may be verified through the Australian Securities and Investments Commission. An employee's medical information will be verified in writing with the employee prior to that medical information being used or supplied to another party, such as a medical assessor. This gives you the opportunity to correct the information and allows us to ensure the information is relevant, accurate, up-to-date, complete, and not misleading prior to the use of the information.

What might be considered 'reasonable steps will depend upon all 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 you if the information is inaccurate or irrelevant
- any opportunities we've already given you to correct inaccuracies
- the effort and cost in checking the information.

10. How we use personal and health information (IPP 10 and HPP 10)

10.1. The principle in brief

We may use personal and health information:

- for the primary purpose for which it was collected
- for a directly related secondary purpose (e.g. Fair Trading might use information from a dispute you lodged in a wider investigation about the trader)
- if we believe the use is necessary to prevent or lessen a serious and imminent threat to life or health
- if it is lawfully authorised or required, or
- for another purpose if you have consented.

10.2. 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 relevant purpose should have been set out in a privacy notice at the time of collection.

We may also use personal and health information for a directly related secondary purpose. A directly related secondary purpose is a purpose that is very closely related to the primary purpose for collection and would closely align with people's expectations around the use of their information. For example, information collected by Fair Trading to mediate a dispute may be accessed and used to investigate possible breaches of legislation or information from a dispute you lodged may be used by NSW Fair Trading in a wider investigation about the trader.

There are several permitted purposes for using health information such as lessening or preventing a serious threat to public safety, managing health services, training, and research.

10.3 How we use personal and health information of employees

If you are a DCS 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 access to any of your own 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 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 employee 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. How we disclose personal and health information (IPP 11 and HPP 11)

11.1. The principle in brief

We may disclose your information if:

- you have consented
- the information is not 'health information' or 'sensitive information' (see point 12 below for a definition of 'sensitive information' and how it is handled), and you have been made aware that the information is likely to be disclosed to the recipient
- the information is not 'health information' or 'sensitive information', the disclosure is directly related to the purpose for which the information was collected, and we have no reason to believe you would object to the disclosure
- if it is lawfully authorised or required
- if it is reasonably necessary to lessen or prevent a serious threat to health
- 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 your reasonable expectations.

11.2. How we apply this principle

We may disclose information we are lawfully authorised or required to disclose, such as where a public register is required to be kept by law.

Other disclosures we make will be appropriately related to the purpose for which the information was collected, or we will have your consent. We may also disclose personal and health information to secondary service providers, such as consultants or investigators, where it is lawful and necessary for carrying out our functions.

We also disclose personal information to other government agencies where it is lawful. For example, under section 13AA of the *Ombudsman Act 1974*, the NSW Ombudsman can request information from a public authority and the relevant provisions of the PPIP Act and HRIP Act do not apply to the agency's response to such a request.

When we are required to disclose information between DCS divisions or with other public sector agencies, we will do so in accordance with the privacy laws.

12. Stricter rules apply to specific information (IPP 12 and HPP 14)

12.1. The principle in brief

Disclosing sensitive information (e.g. your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership 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.

Disclosing personal or health information to someone outside of NSW, or to a Commonwealth agency, is only permitted in limited circumstances as set out in the legislation.

12.2. How we apply this principle

We make every effort to minimise the amount of information we collect about your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities. Where this information is collected, it is treated with the highest protection wherever possible.

We only disclose personal or health information to someone outside NSW, or to a Commonwealth agency, if any of the following applies:

- they are subject to a law, scheme or contract that upholds principles substantially like the NSW IPPs or HPPs
- you have consented
- if it is necessary for a contract with you (or in your interests)
- if it will benefit you and it is impracticable to obtain your consent, but we believe you would be likely to give your consent
- the disclosure is reasonably believed by the relevant division or business unit to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of you or another person
- we have taken reasonable steps to ensure the information won't be dealt with inconsistently with the IPPs or HPPs. For example, where we have bound the recipient by contract to privacy obligations equivalent to the principles, or
- if it is permitted or required by legislation or any other law.

We administer many laws that have equivalent laws in other states and territories. We will therefore liaise

with agencies in other parts of Australia when it is lawful and necessary for carrying out our functions, such as verifying a person's licence status or compliance background in, or for, another state or territory.

13. How we use unique identifiers and linkage of health records (HPP 12, 13 and 15)

13.1. The principle in brief

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.

13.2. How we apply this principle

People and Culture may collect health information to manage cases of injured employees and to investigate workplace incidents. Where health information has been gathered to case manage an injured employee, 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.

Other business units may inadvertently collect health information, even though it is not sought. For example, a person's medical condition may be disclosed to NSW Fair Trading during the mediation of a dispute to explain an absence from the mediation or the inability to complete an action in response to the dispute. When this sort of information is collected, it is not given any separate identifier and is not included in any health records linkage system.

When the 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 2. Some of the key situations where collection, use or disclosure of information is exempted from 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.

Information published on public registers (Part 6 of the PPIP Act)

A public register is a register of information that is publicly available or open to public inspection. If you hold an authority that is required to be published on a public register such as a building licence, some of your personal information will be publicly available, such as your name, address, and any conditions placed on your licence.

Some of our public registers that may disclose personal information are:

- Conveyancers licence check
- Tradesperson and contractor licence check Property services licence check
- Motor industry licence and certificate check
- Accommodation registers (retirement villages, boarding houses, residential parks)
- NSW Incorporated Associations Register
- Torrens title register
- General register of deeds
- Water access licence register
- Asbestos assessor register.
- Loose-fill asbestos insulation register
- Register of disciplinary decisions (BPB)
- Find a certifier (BPB)
- Swimming Pool Register
- Lotteries (Trade Promotions Lottery and Games of Chance)
- Owner Builder Permits
- Register of Co-operatives
- Register of Co-operative Housing and Starr-Bowkett Societies
- Register of Limited and Incorporated Limited Partnerships
- Register of Solicitor Corporations (register closed to new solicitor corporations in December 2000).

The above list is not comprehensive. If you are unsure whether information you have provided to DCS may appear on a public register, please contact us and we can clarify this for you.

We only disclose personal information kept in the above registers in accordance with what is required or permitted under the relevant laws.

If you have any specific concerns about your personal information being on a public register, you can contact the relevant business area within DCS or privacy@customerservice.nsw.gov.au. Any request for your information to be suppressed from a public register must be in writing, must provide reasons for the request, and should also include any evidence, such as a copy of a police report or apprehended violence order.

In making any decision to suppress your information, we will balance your rights with the public interest in maintaining public access to the information, in accordance with legal requirements.

The Australian Criminal Intelligence Commission

Where necessary, DCS also undertakes police checks with the Australian Criminal Intelligence Commission (ACIC). 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 employees 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 and 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 E: Privacy and other legislation relating to personal and health information

Refer to Appendix 1 for further details.

Privacy legislation (NSW, Commonwealth and relevant international)

- *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 2019*
- *Health Records and Information Privacy Regulation 2017*
- Codes of Practice, Directions and Statutory Guidelines made under the PPIP and HRIP Acts
- *General Data Protection Regulation (EU)* (GDPR)
- *Privacy Act 1988 (Cth)* (Privacy Act)
- The Privacy (Tax File Number) Rule 2015 (Cth) (TFN Rule)

Other relevant legislation

- *Crimes Act 1900 (NSW)*
- *Data Sharing (Government Sector) Act 2015 (NSW)*
- *Government Information (Public Access) Act 2009 (NSW)* (GIPA Act)
- *Government Information (Public Access) Regulation 2018*
- *Government Information (Information Commissioner) Act 2009 (NSW)* (GIIC Act)
- *Independent Commission Against Corruption Act 1988 (NSW)*
- *Public Interest Disclosures Act 1994 (NSW)* (PID Act)
- *State Records Act 1998 (NSW)*
- *State Records Regulation 2015*
- *Workplace Surveillance Act 2005 (NSW)*
- *Taxation Administration Act 1996 (NSW)*
- *Fair Trading Act 1987 (NSW)*

PART F: Policies affecting processing of personal and health information

- *DCS Code of Ethics and Conduct*
- *DCS Proof of Identity (POI) Requirements Policy*
- *DCS Information and Data Governance Framework*
- *DCS Records Management Policy*
- *DCS Privacy Management Framework*
- *DCS Information Security Policy*
- *DCS Standard: Reducing the emailing of sensitive information and attachments*
- *DCS Standard: Documenting data flows*
- *DCS Standard: Identification of 'crown jewels'*

PART G: How to access and amend personal information

In most 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.

We must provide access to or amend personal or health information without excessive delay and without expense. We do not charge any fees to access or to amend personal or health information unless you are lodging a formal application under the GIPA Act (see part below).

Formal and informal requests

Informal requests

An informal request simply means that you contact the relevant business unit within DCS, or the DCS 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 business unit within DCS directly if you are trying to access or amend your information. You can also contact the DCS Privacy Officer.

In many cases, the relevant business unit within DCS will be able to amend your personal or health information on the spot, but we may require something in writing from you to safeguard 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 at: https://www.nsw.gov.au/customer-service/who-we-are/access-to-information

No fee is required if you are requesting information under the PPIP or HRIP Acts, however GIPA applications will require the application fee of $30 to be paid.

Formal requests for your personal or health information (whether you are a member of the public or an employee) should be sent to the DCS Privacy Officer.

The Office of the Privacy Commissioner, within the IPC, can also provide help and guidance about your rights to access your personal and health information.

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 can 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 whether personal information will be revealed, as well as any breach of the IPPs and HPPs, as public interest considerations against disclosure.

PART H: 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 and/or amend your personal or health information, we encourage you first to discuss any concerns with the employee or business unit dealing with your information (if known).

Any person may make a complaint:

- By making a general privacy complaint to DCS
- By applying to DCS for an 'internal review' of the conduct they believe breaches an IPP and/or an HPP, which will lead to DCS making findings and may result in some action being taken by DCS
- Directly to the NSW Privacy Commissioner, which may lead to a conciliated outcome.

General privacy complaints

General privacy complaints may include customers raising concerns (either in writing or verbally), to the DCS Privacy Officer, for example, around DCS's processes for handling their information, DCS's handling of a privacy breach or perceived miscommunication.

There are no external review rights to the NSW Civil and Administrative Tribunal (NCAT) at the conclusion of a general privacy complaint.

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

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 employee or division dealing with your information (if known). You can also contact us by email at privacy@customerservice.nsw.gov.au.

The following general principles are relevant to applications for internal review of privacy complaints:

- you may apply to DCS for an 'internal review' of the conduct you believe breaches an IPP or HPP, or you may make a privacy complaint directly to the NSW Privacy Commissioner. For explanation of how we apply the IPPs and HPPs, check out 'Part D: How we manage personal and health information'
- complaints to the Privacy Commissioner can only result in a conciliated outcome, rather than a binding determination
- you cannot seek an internal review for an alleged/potential breach of someone else's privacy, unless you are an authorised representative of the other person
- an application for an internal review must be made within six months from when you first become aware of the conduct you are concerned about (in limited circumstances we may consider a late application for internal review).

See Part J for how to contact the IPC.

How to apply for internal review

Requests for internal review should be sent to privacy@customerservice.nsw.gov.au and needs to:

- be in writing
- be addressed to DCS or the division within DCS to which the complaint relates
- include a return address in Australia, and
- be lodged with the agency 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 a resource. This can be downloaded from their website at www.ipc.nsw.gov.au. Although we encourage you to use 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.
- The internal review will be conducted by a DCS Privacy Team Officer, or by another person who:
  - Was not involved in the conduct, which is the subject matter of the complaint, and
  - Is an employee or an officer of DCS, 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 NCAT. More information on external reviews is provided below.
- We will follow the Privacy Commissioner's Internal Review Checklist (available at ipc.nsw.gov.au) and consider 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 DCS as part of the internal review process.
- In deciding, we may:
  - take appropriate remedial action
  - make a formal apology to you
  - implement administrative measures to prevent the conduct occurring 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 as soon as practical following the completion of the review and 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 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 decision. See Part J for how to contact the IPC.

External Review

If you are unhappy with the outcome of the internal review, you can apply to NCAT to review the decision (an “external review”). Generally, you have 28 days from the date of our internal review decision to seek the external review. You may also apply to NCAT to conduct an external review if we have not completed your internal review within 60 days.

NCAT may make orders requiring DCS 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 DCS to pay damages if the applicant has suffered financial loss or psychological or physical harm because of the conduct.

PART I: Strategies for implementing and reviewing this plan

This edition reflects a review undertaken in March 2021.

Promoting this Plan

Public awareness

This 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.

We aim to promote public awareness of this plan by publishing the plan on our website in a format that is accessible to the widest possible audience, regardless of technology or ability.

DCS 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 an everyday reference point for our privacy management practice.

DCS employees and contractors

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

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

Reviewing this Plan

Our plan will be reviewed at a minimum every two years, but more frequently when legislative, administrative, or systemic changes occur that affect the way we manage the personal and health information we hold.

If you have any feedback on this document please contact the DCS Privacy Officer: by mail at GPO Box 7057 Sydney NSW 2001, by phone to 13 77 88, or by email to privacy@customerservice.nsw.gov.au.

PART J - Contacts

DCS's Privacy Team

For further information about this plan, the personal and health information we hold, or if you have any questions or concerns, please feel free to contact the DCS Privacy Team:

Phone: 13 77 88
Email: privacy@customerservice.nsw.gov.au
Web: www.customerservice.nsw.gov.au
Mail: DCS Privacy Officer
Governance, Risk and Performance, Corporate Services
GPO Box 7057
Sydney NSW 2001
Office: McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

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: Information and Privacy Commission NSW
GPO Box 7011
Sydney NSW 2001

Office: McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

The NSW Civil and Administrative Tribunal (NCAT)

NCAT's contact details are:

Phone: 1300 006 228 and select Option 3 for all Administrative and Equal Opportunity Division enquiries
Email: aeod@ncat.nsw.gov.au
Web: 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

Appendix 1: Other related laws

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

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

Data Sharing (Government Sector) Act 2015 (NSW) 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.

Fair Trading Act 1987 (NSW) regarding the regulation of the supply, advertising and description of goods and services in NSW. Includes various provisions relating to the disclosure and sharing of information, for example, the publication of certain information for public access.

Government Information (Public Access) Act 2009 (NSW)* (GIPA Act) and *Government Information (Public Access) Regulation 2018

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,
please contact DCS's GIPA team at gipa@customerservice.nsw.gov.au or on (02) 9219 3700.

***General Data Protection Regulation (EU)* (GDPR)**

Although a European privacy law, the GDPR is designed to have extra-territorial reach. The GDPR came into effect on 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 (NSW)* (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 an 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 J for how to contact the IPC).

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

Privacy Act 1988 **(Privacy Act)**

Under the Privacy Act, the Australian Information Commissioner has several monitoring, advice, and assessment related functions regarding the handling of tax file numbers (TFNs).

The **Privacy (Tax File Number) Rule 2015 (TFN Rule)** issued under s 17 of the Privacy Act regulate the collection, storage, use, disclosure, security, and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

The TFN Rule is legally binding. A breach of the TFN Rule is an interference with privacy under the Privacy Act. Individuals who consider that their TFN information has been mishandled may make a complaint to the Office of the Australian Information Commissioner (OAIC).

Public Interest Disclosures Act 1994 (NSW) **(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 (NSW) **and** ***State Records Regulation 2015*** regarding the management and destruction of records.

Taxation Administration Act 1996 (NSW) regarding administration and enforcement of taxation laws. Division 3 of this Act includes secrecy provisions, including that a person who is or was a tax officer must not disclose any information obtained under or in relation to the administration of a taxation law, except as permitted under this Act.

Workplace Surveillance Act 2005 (NSW) regarding the regulation and legal use of camera, audio, computer surveillance and geographical tracking.

Appendix 2: 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 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 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 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 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 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 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
- where the provisions of GIPA impose conditions or limitations (however expressed)

Access – IPP 7 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 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 GIPA that impose conditions or limitations (however expressed)

Accuracy – IPP 9 and HPP 9

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

Use – IPP 10 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 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 3: Guide to drafting privacy collection notices

Where DCS collects personal information from individuals, including for its own internal administrative purposes, it must make those individuals aware of the specified matters.

The following principles guide the drafting of privacy notices within DCS:

- the DCS Privacy Officer must approve the wording and location of all privacy notices
- if the transaction can occur across more than one service channel/entity, the privacy notice should be worded as closely as possible across each channel/entity
- wording should be concise and in plain language
- the notice should clarify what DCS will do with the information, as well as what any other entity or agency will do with the information
- the notice should be given / visible before any data collection begins
- notice can be provided on the paper forms developed by the entity or agency
- for digital transactions, the notice should be given on the landing page for that transaction, even if it also appears later in the process, and
- for digital transactions, if the data is being collected and stored by DCS, the notice should also appear on the first data collection page.

At the end of each privacy notice it should be stated that for further information about privacy, contact the relevant Privacy Officer.

Appendix 4: Detailed list of DCS cluster

The DCS cluster houses individual agencies, offices, entities, and business units that carry out various functions.

Business units of DCS

- *Corporate Services:* provides specialised services for the department including finance, legal, risk, communications, cluster-wide procurement
- *People and Culture:* provides employee services.
- *Office of the Secretary*: provides support and strategy for priority activities of the Secretary or Ministers and high quality, timely advice on Ministerial and Cabinet submissions.

Improving our customer service

- *Office of Customer Service Commissioner*: provides independent advice to the Premier, Cabinet, Ministers and NSW Government agencies and departments on all aspects of customer service.
- *Brand and Digital Communications, Customer Delivery Transformation:* leads internal and external engagement across the Customer Service cluster and for NSW Government. This includes community and employee engagement, marketing and social media and NSW Government brand and digital channels
- *Births Deaths and Marriages*: registers life events in NSW accurately and securely, ensuring the integrity and confidentiality of all records.

Regulation agencies

- *NSW Fair Trading*: safeguards the rights of all consumers and advises business and traders on fair and ethical practice.
- *Professional Standards Authority*: provides regulatory and general support services for the Professional Standards Council with the core purpose to protect Australian consumers by improving professional standards.
- *Office of the Registrar General*: ensures the integrity of the NSW land title system.
- *Office of the Building Commissioner:* improving the quality of construction and restoring trust in the industry through leading the delivery of Construct NSW, in collaboration with the sector.
- *Office of Responsible Gambling:* leads the development of responsible gambling strategy and public policy advice to the NSW Government, and manages programs and initiatives to prevent and reduce gambling harms in the community
- *Office of Racing:* Responsible for the state's thoroughbred, harness and greyhound racing industries, including managing relationships with the three codes' controlling bodies
- *SafeWork NSW*: State's workplace health and safety regulator works to reduce work-related fatalities, serious injuries and illnesses making it easier to do business safely.
- *Liquor & Gaming NSW*: regulates the liquor, gaming, wagering, casino and registered clubs' sectors in NSW, and provides policy advice to government in these spaces.
- *Subsidence Advisory NSW:* responsible for administering the *Coal Mine Subsidence Compensation Act 2017*.

Using analytics, insights and information

- *Data Information and Transformation, Customer Delivery Transformation*: Joins together the NSW Data Analytics Centre, the Data.NSW program, the Behavioural Insights Unit and a newly created Transformation function to deliver evidence-driven sector-wide prioritisation of effort and investment, measurement of customer impact and needs, service and business reform and personalisation of government services including emerging technology..

- *Delivery Unit, Customer Delivery Transformation:* Drives the successful delivery of key Ministerial priorities that aim to make government work better for customers.
- *Innovation NSW*: programs that showcase innovation in government to improve customer outcomes.

Our digital and ICT agencies and businesses

- *Digital Channels, Customer Delivery Transformation:* principally employed in administering the nsw.gov.au website, as well as leading the website consolidation project will consolidate 500 websites across NSW Government onto a single website at nsw.gov.au.
- *Government Technology Platforms, Digital.NSW:* provides cross sector leadership and delivery of ICT infrastructure and service delivery reforms aligned to the NSW Government ICT Strategy.
- *Government Chief Information and Digital Office (GCIDO), Digital.NSW:* leads Digital.NSW which is responsible for driving digital transformation and developing digital capacity within the NSW Government through collaboration across clusters.
- *ICT Digital Investment and Assurance, Digital.NSW:* developed the ICT Assurance Framework to enable NSW to transition towards Digital Government.
- *ICT Digital Sourcing, Digital.NSW:* responds to high priority, ongoing projects and the need to bring teams together in an agile way to achieve more effective delivery.
- *Spatial Services, Digital.NSW:* provides spatial and land information services for NSW
    - *Spatial Operations:* production and maintenance of NSW Foundation Spatial Data
    - *Emergency Information Co-ordination Unit*: ensures the emergency management sector has the best spatial and related data available to deal with multi-agency emergencies, such as terrorism and natural disasters

Other

- *Cyber Security NSW*: provides leadership and coordination in managing risks against cyber threats.

Separate “public sector agencies” covered by the DCS PMP

The following entities which are part of the DCS Cluster are separate “public sector agencies” however clause 6 of the PPIP Regulation means the DCS PMP extends to them and they are not required to have their own PMP and do not have an existing PMP.

- *Long Service Corporation*: provides workers in building, construction and contract cleaning industries a financial reward for long service.
- *NSW Telco Authority*: coordinates radio telecommunication services for the NSW Government.
- *Rental Bond Board:* administers the Board's day to day functions, providing rental bond lodgement, custody, refund and information services.
- Spatial Services: provides spatial and land information services for NSW.
    - *Surveyor General of NSW:* implements and monitors standards for the survey industry in NSW.
    - *Board of Surveying and Spatial Information (BOSSI):* sets and regulates competency standards for surveyors in NSW.
    - *Geographical Names Board:* the official body for naming and recording details of places and geographical names in the state of New South Wales.

Separate “public sector agencies” which are not covered by the DCS PMP

The following entities and/ or divisions are part of the DCS Cluster however as separate “public sector

agencies" under the PPIP Act they are either required to have their own PMP or have an existing PMP.

- *Hardship Review Board:* an independent body established under the *State Debt Recovery Act 2018* which reviews applications to alter a fine, fee, tax or duty imposed by Revenue NSW.
- *Independent Pricing and Regulatory Tribunal*: provides independent regulatory decisions and advice to protect and promote the ongoing interests of consumers and taxpayers
- *Independent Liquor and Gaming Authority (ILGA*): a statutory decision-maker responsible for a range of casino, liquor, registered club and gaming machine regulatory functions including determining licensing and disciplinary matters under the gaming and liquor legislation.
- *Information and Privacy Commission NSW (IPC)*: administers legislation dealing with privacy and access to government held information in NSW.
- *NSW Architects Registration Board:* administers the *Architects Act 2003*, the legislation regulating architects in NSW. The Board's key role is to protect consumers of architectural services by ensuring that architects provide services to the public in a professional and competent manner and accrediting architectural qualifications for the purpose of registration and promoting a better understanding of architectural issues in the community.
- *Greyhound Welfare and Integrity Commission (GWIC)*: the independent regulator established to administer animal welfare and governance functions within the greyhound industry.
- *Office of the Independent Review Officer (IRO):* re-established to deal with complaints from persons injured in motor vehicle accidents under the *Personal Injuries Commission Act 2020* (PICA), the Office of the IRO is to become a separate Public Sector agency, the IRO' s jurisdiction is to be expanded to deal with complaints from persons injured in motor vehicle accidents.
- *Personal Injury Commission (PIC):* a "one-stop shop" in dispute resolution for road and workplace injuries in NSW which consolidates the dedicated dispute resolution services of the Workers Compensation Commission (WCC) and SIRA into a single, independent tribunal.
- *Service NSW*: a separate public sector agency that delivers customer-facing transactions for many government agencies, providing a single point of contact for customers for a range of licensing and transactional services.
- *State Insurance Regulatory Authority (SIRA):* responsible for the regulatory functions for workers compensation insurance, motor accidents compulsory third party insurance and home building compensation.
- *Long Service Corporation*: provides workers in building, construction and contract cleaning industries a financial reward for long service.
- *Revenue NSW*: a standalone division reporting directly to the Secretary, which collects revenues, administers grants and recovers debts.

Appendix 5: List of DCS Privacy Officer contacts

If your privacy complaint concerns the conduct of one of the below entities, or you believe your personal information may be held by one of these agencies, please contact the relevant Privacy Officer directly as follows:

Agency	Contact details
Safework NSW	**Email:** **privacy**@**safework**.**nsw**.gov.au **Phone:** 13 10 50
Revenue NSW	Email: RNSWprivacy@revenue.nsw.gov.au
Hardship Review Board	Email: RNSWprivacy@revenue.nsw.gov.au
Independent Pricing and Regulatory Tribunal (IPART)	Email: ipart@ipart.nsw.gov.au Phone: (02) 9290 8400
Independent Liquor and Gaming Authority (ILGA)	Email: contact.us@liquorandgaming.nsw.gov.au Phone: 1300 024 720
Information and Privacy Commission (IPC)	Email: ipcinfo@ipc.nsw.gov.au Phone: 1800 472 679
NSW Architects Registration Board	Email: mail@architects.nsw.gov.au Phone: (02) 9241 4033
Office of the Greyhound Welfare and Integrity Commission	Email: emailus@gwic.nsw.gov.au Phone: 13 49 42
Office of the Independent Review Officer (IRO)	Email: complaints@iro.nsw.gov.au Phone: 13 94 76
Personal Injury Commission (IPC)	Email: gipa@wcc.nsw.gov.au Phone: 1800 742 679
Service NSW	Email: privacy@service.nsw.gov.au Phone: 13 77 88
State Insurance Regulatory Authority (SIRA)	Email: privacy@sira.nsw.gov.au
Long Service Corporation (LSC)	Web form: https://www.longservice.nsw.gov.au/contact-us/feedback