Department of Customer Service

DCS Privacy Management Plan

Document number: 1	Version number: 2.5
Date: 15 August 2022	

Contact details

Name: Michael Wright	Position: Manager, Governance (Privacy)
Business Unit: Governance, Risk and Performance	Division: Corporate Services
Phone:	Email: privacy@customerservice.nsw.gov.au

Table of Contents

1. Introduction 4

1.1. About DCS 4
1.1.1. Ministerial Portfolios: 4
1.1.2. Agencies & Business Units: 4
1.1.3. Stakeholders: 4

2. Privacy Management Plan 5

2.1. Scope 5
2.2. Effect of privacy 5
2.3. EmployeesWho the Privacy Management Plan Covers 5
2.3.1. Cluster agencies not covered by this Plan 5
2.4. Responsibilities of employees and others 6
2.4.1. Responsibilities of the DCS Privacy Officer 6
2.4.2. Responsibilities of the DCS Privacy Team 6
2.5. Plan Review Frequency 7

3. Legislative & Policy Framework 7

3.1. Privacy legislation 7
3.2. Other legislation 7
3.3. Relevant policy documents 7

4. Personal and Health Information 8

4.1. What is personal information 8
4.1.1. What is NOT personal information? 8
4.2. What is health information 8
4.2.1. What is NOT health information? 9
4.3. Types of personal and health information DCS holds 9
4.3.1. Customers 9
4.3.2. Employees 10
4.4. Business records 10
4.5. Information management systems 10
4.6. Use of cookies 10
4.7. Links to other sites 11

5. Management of Personal and Health Information 11

5.1. Collection 11
5.1.1. Collection for a lawful purpose (IPP 1 and HPP 1) 11
5.1.2. Direct collection (IPP 2 [PPIP s9] and HPP3) 11
5.1.3. Requirements when collecting information (IPP 3 [PPIP s10] and HPP 4) 12
5.1.4. Relevant (IPP 4 [PPIP s11] and HPP 2 13
5.2. Retention and security (IPP 5 [PPIP s12] and HPP 5) 13
5.2.1. Transparency (IPP 6 [PPIP s13] and HPP 6) 15
5.2.2. Access to personal and health information (IPP 7 and HPP 7) 15
5.2.3. Alterations to personal and health information (IPP8 and HPP 8) 16
5.3. Use 17
5.3.1. Accuracy (IPP 9 [PPIP s16] and HPP 9) 17
5.3.2. Limited use (IPP 10 [PPIP s17] and HPP 10) 17
5.4. Disclosure 18
5.4.1. Disclosure (IPP11 &12 and HPP11 &14) 18
5.4.2. Identifiers (HPP 12) 19
5.4.3. Anonymity (HPP 13) 19
5.4.4. Linkage of health records (HPP 15) 19
5.5. Exemptions on how we manage personal and health information 20
5.5.1. When the principles do not apply (IPPs and HPPs) 20
5.6. Information published on public registers (Part 6 of PPIPA) 21

5.7. The Australian Criminal Intelligence Commission 21
5.8. Statistical information 21

6. How to Access and Amend Personal Information 22

6.1. Informal requests 22
6.2. Formal requests 22
6.3. Limits on accessing or amending other people's information 22

7. Your Review and Complaint Rights 23

7.1. Informally 23
7.2. Your Right of Internal Review 24
7.2.1. Process 24
7.2.2. Timeframes 25
7.3. Your Right of External Review 25
7.4. Complaints to the Privacy Commissioner 25

8. Strategies for Compliance and Continuous Improvement 26

8.1. Policies and procedures 26
8.2. Promoting privacy awareness 26
8.3. Review and continuous improvement 26
8.4. Directions of the Privacy Commissioner to modify PPIPA or HRIPA 26
8.5. When can information be shared with others for analysis 27
8.6. When should a Privacy Threshold Assessment and Privacy Impact Assessment be done? 27
8.7. Notification of a Data Breach 28

9. Key Contacts 28

9.1. DCS Privacy Team 28
9.2. The NSW Information and Privacy Commission (IPC) 28
9.3. The NSW Civil and Administrative Tribunal (NCAT) 28
9.4. Relevant Agency Privacy Lead Contacts 29

10. Resources – Other Related Laws 31

This section contains a summary of other laws that may have an impact on the way we handle personal and health information 31

11. Glossary of Terms 32

12. Document Control 34

12.1. Document Approval 34
12.2. Document Version Control 35

1. Introduction

This is the Privacy Management Plan (DCS PMP) for the NSW Department of Customer Service (DCS). Our DCS PMP shows what measures we take to comply with the *Privacy and Personal Information Act 1998 (NSW)* *(PPIPA)* and the *Health Records and Information Privacy Act 2002 (NSW)* *(HRIPA)* to protect personal and health information.

The 12 Information Protection Principles (IPPs) in the PPIPA and the 15 Health Information Privacy Principles (HPPs) in the HRIPA provide detail on how to collect, store, use, disclose, provide you with access to, and/or amendment of, your personal and/or health information as well as destroy the information when it's no longer required.

1.1. About DCS

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 provide services to citizens and do business in NSW.

1.1.1. Ministerial Portfolios:

Our lead cluster minister is the Minister for Customer Service and Digital Government. Our other Ministers are the Minister for Small Business and Fair Trading, and the Minister for Finance and Employee Relations.

1.1.2. Agencies & Business Units:

DCS sets the strategic direction for customer service and works in partnership with a number of government agencies and business units to deliver customer-centric outcomes for the community.

DCS is the central department within the customer service cluster. There are over 30 agencies, divisions and business units within the cluster. Further information about our structure, functions and activities is available on our website.

1.1.3. Stakeholders:

We collect, hold, use and disclose personal and health information for the purpose of carrying out these functions and activities. To do this, we work with many stakeholders such as:

- 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.

2. Privacy Management Plan

The DCS Privacy Management Plan (DCS PMP) explains how we manage personal and health information under NSW privacy laws.

We have obligations to protect the privacy rights of customers, employees and members of the public. We take these responsibilities seriously.

In particular, we are required to take reasonable steps to enable you to ascertain whether we hold personal or health information relating to you, the nature of that information, the main purposes for which it is used and your entitlement to access and amend that information.

This DCS PMP:

- illustrates our commitment to respecting the privacy rights of customers, employees and members of the public, and enhances the transparency of our operations
- provides our employees and contractors with the necessary knowledge and skills to manage personal and health information appropriately
- supports the development of policies and procedures to ensure our compliance with privacy laws
- meets the requirements for us to have a plan under s33 of PPIPA.

Further information and research in relation to privacy is available on the Information and Privacy Commission (IPC) website: http://www.ipc.nsw.gov.au/.

2.1. Scope

This DCS PMP applies to our treatment of all personal and health information, whether it relates to a customer, employee or another person (such as contractor).

2.2. Effect of privacy

DCS, as a 'public sector agency', must comply with all the applicable privacy principles. Where DCS uses personal or health information internally, this will be a 'use' for privacy purposes. Where DCS provides information to another person or body, including an agency within the cluster, this will constitute a 'disclosure' for privacy purposes.

2.3. Employees Who the Privacy Management Plan Covers

This DCS PMP covers the majority of DCS divisions and agencies. Some divisions or agencies, for example NSW Fair Trading, will also have a Privacy Code of Practice.

2.3.1. Cluster agencies not covered by this Plan

Privacy law generally requires that each public sector agency has its own Privacy Management Plan. The following cluster agencies are not part of DCS for privacy purposes and are therefore required to have their own Privacy Management Plan. These include:

- Independent Pricing and Regulatory Tribunal (IPART)
- Information and Privacy Commission (IPC)
- NSW Architects Registration Board
- Office of the Independent Review Officer (IRO)
- Personal Injury Commission (PIC)

- Service NSW
- State Insurance Regulation Authority (SIRA)

2.4. Responsibilities of employees and others

All DCS employees and persons engaged by DCS are required to comply with PPIPA and HRIPA, including relevant privacy principles as set out in each Act. Additionally, they are required to comply with the DCS Code of Ethics and Conduct and the DCS Conflicts of Interest Policy.

This DCS PMP is intended to assist these employees and persons to understand and comply with the obligations under those Acts.

Employees suspected of conduct that breaches the PPIPA, HRIPA or relevant privacy principles 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.

Under s62 of PPIPA:

It is a criminal offence, with a maximum penalty of 100 penalty units or imprisonment for 2 years, or both, for any employees (or former employees) of DCS to intentionally use or disclose any personal information about another person, to which the employee has or had access in the exercise of his or her official functions, except as necessary for the lawful exercise of his or her functions.

2.4.1. Responsibilities of the DCS Privacy Officer

The *Executive Director, Governance, Risk and Performance* has specific responsibilities for this DCS PMP as the role is the DCS Privacy Officer, responsible for providing governance services to a portfolio of divisions.

The DCS Privacy Officer leads a dedicated DCS 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.

The DCS Privacy Officer may also work with the Privacy Leads across the cluster, where appropriate.

2.4.2. Responsibilities of the DCS Privacy Team

The DCS Privacy Team is responsible for the following:

- Developing, co-ordinating and embedding the:
  - Privacy Management Plan (this DCS PMP)
  - Privacy Management Framework (the DCS PMF)
  - Privacy Partners Network (Community of Practice)
  - Reporting
- Periodically reviewing and updating the DCS online employees training and information resources.
- Consulting with the Privacy Commissioner on high-risk programs or incidents.
- Ensuring relevant privacy documents are consolidated and made available through DCS's website.

- Coordinating and, where appropriate, investigating privacy incidents, breaches and complaints.

The DCS annual report includes a statement of the actions taken to ensure compliance with the requirements of PPIPA. The statement also provides statistical details of any review conducted, or conducted on our behalf, under PPIPA. DCS' annual reports can be found on our website: https://www.nsw.gov.au/customer-service/publications-and-reports.

2.5. Plan Review Frequency

We will review this DCS PMP every year or earlier if any legislative, administrative, or systemic changes affect how we need to manage personal and health information.

3. Legislative & Policy Framework

3.1. Privacy legislation

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

- *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIPA)
- Privacy and Personal Information Protection Regulations 1998
- *Health Records and Information Privacy Act 2002 (NSW)* (HRIPA)
- Health Records and Information Privacy Regulation 2006

3.2. Other legislation

Our handling of personal and health information may be regulated or otherwise affected by other legislation, such as:

- *Crimes Act 1900 (NSW)**
- *Criminal Records Act 1991 (NSW)*
- *Data Sharing (Government Sector) Act 2015** *Government Information (Public Access) Act 2009 (NSW)**
- *Government Information (Information Commissioner) Act 2009 (GIIC Act)**
- *Independent Commission Against Corruption Act 1988**
- *Privacy Act 1988* (Cth)*
- *State Records Act 1998 (NSW)*i*
- State Records Regulation 2010 (NSW)*
- *Workplace Surveillance Act 2005 (NSW)*
- *Surveillance Devices Act 2007 (NSW)*
- *Ombudsman Act 1974 (NSW)*
- *Public Interest Disclosures Act 1994 (NSW)**
- *Telecommunications Act 1997*
- *Telecommunications (Interception and Access) Act 1979 (Cth)*

*Refer to Section 10 for a summary and link to the relevant act.

3.3. Relevant policy documents

DCS has developed the following policy documents to ensure compliance with the privacy legislation, to manage privacy risks and deal with other matters that DCS considers relevant in relation to privacy and protection of personal and health information held by DCS:

DCS Privacy Management Framework (the DCS PMF) is an internal guideline for DCS employees on how the principles and aims of the DCS PMP are embedded in the agency's integrated policies, operating plans, business processes and work practices.

DCS Data Incident Response Plan (the DCS DIRP) outlines the processes and methods by which DCS employees can identify, contain, assess, respond to, and remediate suspected, potential, or actual data incidents, including breaches. The DCS DIRP has been formulated in accordance with the Commonwealth Privacy Act's Notifiable Data Breach Scheme and the proposed NSW Mandatory Notifiable Data Breach Scheme set out in the *Privacy and Personal Information Protection Amendment Bill 2021* (NSW).

DCS Risk Management Policy sets out the principles and requirements of our risk management approach for all risk categories, including privacy.

DCS Code of Ethics and Conduct helps all us to understand and know who we are, what we stand for and how we operate with each other, our sector colleagues and our customers. It outlines the responsibilities of our employees in protecting privacy in the course of their duties. All employees are provided with a copy of the Code and are regularly reminded of their obligations.

4. Personal and Health Information

4.1. What is personal information

Personal information is defined in s4 of PPIPA as:

'*information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'*.

Personal information is broadly defined and includes information or an opinion that identifies a person or that would allow a person's identity to be discovered, using moderate steps, including by reference to other information. Information which, on its face value, does not appear to identify an individual will still be personal information if the information can be combined with other information, including information held by DCS, to identify the person. For example, a customer reference number on its own may not be personal information but combined with other information it may be.

4.1.1. What is NOT personal information?

There are certain types of information that is not considered personal information. These are outlined at s4(3) and 4A of PPIPA.

This means that the IPPs do not apply to our handling of certain types of information. These include:

- Information about an individual who has been dead for more than 30 years
- Information about an individual that is contained in a publicly available publications (for example information provided in a newspaper or a court judgement available on the internet).
- Information that has been de-identified is not personal information, provided it is not capable of being re-identified (including by DCS).

4.2. What is health information

Health information is a specific type of personal information that is defined in s6 of HRIPA as:

- Personal information that is also information or an opinion about:
    - An individual's physical or mental health or disability
    - An individual's express wishes about the future provision of health services to themselves
    - A health service provided, or to be provided, to an individual.
- Other personal information collected to provide a health service
- Other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances
- Genetic information that is or could be predictive of the health or a person or their relatives or descendants
- Healthcare identifiers.

4.2.1. What is NOT health information?

As with personal information, there are certain types of information which are not considered health information. These are outlined in s5(3) of HRIPA and include some of the types of the information listed in section 4.1.1 above.

4.3. Types of personal and health information DCS holds

DCS undertakes a diverse range of functions and activities. The collection of customer information is a central part of many of these functions and activities. We also have substantial obligations in respect of maintaining personal files and records of our employees.

As a consequence, we hold a large amount of personal and health information about customers and employees in a number of different locations and formats.

4.3.1. Customers

To fulfill our various functions and activities, we hold a broad range of personal and/or health information obtained through our business areas. These include the NSW tax system, fair trading or home building disputes, licences and certificate applications. The following personal and health information may be collected, depending on the specific needs of the customer and the agency:

- Name and contact details
- Wages/Income details
- Tax file numbers
- Home address
- Insurance claims history
- Job specifications and status
- Financial and bank accounts
- Medical certificates and injuries
- Date of birth
- Correspondence
- Payroll tax
- Criminal records
- Insurance information
- Land tax
- Bankruptcy information
- Signatures
- Complaints
- Interpreter use
- Employment details
- Investigations
- Land title information
- Compliance history

The above list is not exhaustive.

We may also hold other personal or health information provided by customers for a

range of specific functions of our divisions. We may collect information electronically, in hard copy, via email or over the phone.

4.3.2. Employees

For various reasons, such as leave management, workplace health and safety and operational requirements, DCS keeps employees' records including:

- Documents related to the recruitment process
- Personal contact details and emergency contact details (including telephone number, postal and email address)
- Date of birth
- Financial information (such as salary, bank account information, tax file number)
- Personnel information (such as attendance records, leave balances, educational and professional qualifications, training records)
- Background information (such as criminal history, ethnic background, disability)
- Health information (including medical certificates, reports and files, fitness for duty assessments and vaccination status)
- Statements and opinions
- Audio recordings of telephone conversations and interviews
- Photographs/footage
- Injury management information such a workplace injury, workers compensation claims and payments and return to work plans.

This information is collected directly from employees and is managed in accordance with the provision of PPIPA.

4.4. Business records

DCS maintains business records that contain personal information including contact details for public officials in other government entities, as well as third party organisations. Contacts with other government and third-party entities and individuals may include personal information. This information is managed in accordance with the provisions of PPIPA.

4.5. Information management systems

DCS uses a variety of information management systems including paper-based filing systems and electronic records forming part of a secure computerised database.

We follow strict rules in storing personal information in all formats to protect personal information from unauthorised access, loss or other misuse.

4.6. Use of cookies

A 'cookie' is a small data file placed on your machine or device which lets DCS identify and interact more effectively with your computer. Cookies are industry standard and are used by most websites, including those operated by DCS. Cookies can facilitate a user's ongoing access to and use of a website. Cookies allow DCS to customise our website to the needs of our users. If you do not want information collected through the use of cookies, there is a simple procedure in most browsers that allows you to deny or accept the cookie feature. However, cookies may be necessary to provide you with some features of our online services via the DCS website.

4.7. Links to other sites

DCS may provide links to third party websites. These linked sites may not be under our control and DCS is not responsible for the content or privacy practices employed by those websites. Before disclosing your personal information on any other website, we recommend that you carefully read the terms and conditions of use and privacy statement of the relevant website.

5. Management of Personal and Health Information

The section provides an overview of how DCS complies with the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) when we handle the personal and health information of our customers, employees and members of the public.

In addition to our obligations under the IPPs and HPPs, our employees' records are administered in accordance with the NSW Government Public Service Commission Handbook.

If you require further information about how privacy laws apply to a particular situation, please contact the employee or business area dealing with the information or as detailed on the 'contact us' page.

5.1. Collection

5.1.1. Collection for a lawful purpose (IPP 1 and HPP 1)

We will only collect personal and health information if:

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

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

We only ask for personal and health information that is reasonably necessary to the task at hand and is required for our functions and activities.

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

5.1.2. Direct collection (IPP 2 [PPIP s9] and HPP3)

We generally collect personal or health information directly from the person concerned.

We will only collect information from a third party where:

- The person has authorised collection of the information from someone else
- The person is under 16 years of age – in which case we may instead collect personal information from the person's parent or guardian
- In the case of health information, it would be unreasonable or impracticable to collect information from an individual.

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.

5.1.3. Requirements when collecting information (IPP 3 [PPIP s10] and HPP 4]

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

- the fact that the information is being collected
- what it will be used for
- what other parties (if any) routinely receive this type of information from us
- whether the information is required by law (and if so, by which law) or is voluntary
- what the consequences will be for the person if they do not provide the information to us
- that they have a right to access and/or correct their personal and health information, which is held by us,
- the name and contact details of the agency collecting and holding the information.

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

Generally, we provide this notification by way of a 'privacy notice' that is included in application forms, web page, recorded message or in a verbal notice (via phone scripts) at the time the personal or health information is collected, or as soon as we can afterwards.

If your information is to be used for a purpose other than what it is collected for, your consent is required to be specifically sought. This consent will be in addition to any privacy statement or collection notice.

Consent means 'express consent or implied consent' and should:

- adequately inform you prior to giving consent
- be provided voluntarily
- be current and specific
- consider your capacity to understand and communicate your consent.

You can provide express consent either orally or in writing.

Implied consent arises where it may be reasonable inferred in the circumstances from your conduct/actions. Silence is not consent.

'Voluntarily' should be understood to mean that there was a genuine opportunity for you to provide or withhold your consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower your will.

Opting out is not an advisable way to seek consent. However, there are times when this is our most appropriate action. If an opt-out is used, the following factors, where relevant, must be met:

- the opt-out option is clearly and prominently presented

- it is likely the information about collection, use or disclosure and opt-out was read (it forms part of a form filled out by you, for example)
- information about the implications of not opting-out was given
- the opt-out option is freely available and not bundled with other purposes
- it is easy to choose the opt-out, e.g., little or no effort is required to do so
- consequences of failing to opt out are not serious
- if opting-out later, it will appear as if opted-out earlier (as far as practicable).

Notification is not required if the information is not collected directly from the individual, except in the case of health information. In the case of health information, we are obliged to take reasonable steps to ensure the individual is generally aware of the notification matters except in certain circumstances (such as where collection from a third party is necessary or directly relevant and the individual to whom the information relates is unlikely to suffer burden or harm and is not discriminated against and decisions are not made about the individual), or otherwise in accordance with NSW Privacy Commissioner Guidelines[1].

5.1.4. Relevant (IPP 4 [PPIP s11] and HPP 2

When collecting information from an individual, we will:

- *Not collect excessive personal or health information*
- *Not collect personal or heath information in an unreasonable intrusive manner*
- *Ensure that personal and health information collected is relevant, accurate, up-to-date and complete.*

We take reasonable steps to ensure that information we collect from an individual is not unreasonably intrusive or excessive, and is relevant, accurate, up-to-date, and complete. We may also cross reference 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.

To determine what might be reasonable steps, we consider:

- the purpose for which the information was collected
- the sensitivity of the information
- how many people have access to the information
- the importance of the accuracy to the proposed use
- the potential effects for the individual concerned if the information is inaccurate, out-of-date, or irrelevant
- the opportunities to subsequently correct the information
- the ease with which agencies can check the information.

5.2. Retention and security (IPP 5 [PPIP s12] and HPP 5)

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

[1] Statutory guidelines on the collection of health information from a third party are available from http://www.ipc.nsw.gov.au/resources-public-sector-agencies

Where it is necessary for personal and health information to be transferred to a person in connection with the provision of a service, we will take steps to prevent unauthorised use and disclosure of that information.

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

Information is stored in a variety of ways, including in our databases, cloud storage, by third parties and in various physical office locations.

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

Examples of retention and security measures that we have in place include:

- All databases and applications administered by DCS ICT that hold personal or health information have an agreed set of personal information protection controls applied, including user access controls. The control standards are determined by the DCS Privacy Team based on requirements outlined in privacy legislation. They include measures to ensure only people with a reason to have access to the personal or health information can access it. 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, we apply a minimum password standard, including requiring employees to change passwords on a quarterly basis and ensure that passwords are suitably complex.
- Option of Multi-factor authentication (MFA) 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 given when access attempts to confidential systems are made.
- Security audits 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.
- Print on demand (secured printing).
- Implementing and maintaining strong security software across all network components in arrangements for data transmissions (including encryption and password protection where appropriate), back up and storage.
- Implementing and observing a clear desk policy.
- Maintaining and continually improving information security management systems that comply with ISO/IEC 27001:2013 standard.
- Aligning our obligations under the Cyber Security Policy.
- Adopting best practice in electronic and paper records management and complying with our obligations under the *State records Act 1998 (NSW).*

- Keeping information for only as long as necessary.
- When no longer required, destroying information in as secure a manner as appropriate (for example, using secure (locked) recycling bins and shredders).
- where it is necessary for information to be transferred to a third party for the purposes on service provision, developing and executing contract terms that would prevent them from unauthorised use or disclosure of information that we hold.
- Providing mandatory information security awareness training to DCS employees.

Access to electronic record 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 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 (NSW)* and standards issued by State Archives NSW.

In agencies, or 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.

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

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 personal and health information
- the main purpose for which we used your personal or health information
- your entitlement to access your personal and health information.

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 the ‘4.2.3: Requirements when collecting information section), 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.

If you have any questions about the personal and health information we hold about you please contact the employee or business unit dealing with your information. If you are unsure who to contact, refer to the 'contact us' page.

5.2.2. Access to personal and health information (IPP 7 and HPP 7)

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, and we will provide written reasons, if requested.

Members of the public

We encourage you to contact the employee or business unit holding your information if you wish to access it. In some cases, you may be able to access your own personal information by accessing an online account or website.

If you do not know which business unit to contact regarding your request or your request has been denied, please fill out and submit an Application Form - Access or contact us as outlined in the 'contact us' section.

Employees

Employees are able to access their personnel file by making a request to People & Culture hradvice@customerservice.nsw.gov.au.

Files about disciplinary matters and grievances are confidential, and access is generally provided only to the employee to whom the file relates. Generally, employees may inspect files under supervision and will also be able to take photocopies of material on their file.

Access to information under GIPAA

Anyone is able to make an access application under the *Government Information (Public Access) Act 2009* (GIPAA). Sometimes the information that is requested includes personal and health information of other people. There are certain considerations that are considered before any information is released and we may withhold the personal or health information of another person.

For more information about GIPAA or making an access application, please visit our website.

5.2.3. Alterations to personal and health information (IPP8 and HPP 8)

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.

Where practicable, we will notify any other recipients of any changes.

We encourage you to help us keep any information we hold about you accurate, up-to-date, and complete by contacting us with updated information. In some cases, you may be able to access your own personal information by accessing an online account or website.

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.

If the information we hold is accurate, relevant, up-to-date, complete and not misleading but a person still insists on an amendment, we can decline to do so, however we must allow the person to add a statement to our records. For example, it may be appropriate to attach a statement, instead of amending information, for a disputed medical diagnosis or a person with a criminal record maintaining their innocence.

Members of the public

If you do not know which business unit to contact regarding your request or your request has been denied, please fill out and submit an Application Form – Alteration

or contact us as outlined in the 'contact us' section.

Employees

Employees can request amendment of their personal or health information by contacting People and Culture.

We encourage you to keep your personal information up-to-date and accurate, particularly information about your personal contact details, next of kin contact details so that you (or they) can be contacted in an emergency. It is also your responsibility to inform us if you wish to change your bank account details or payment details.

5.3. Use

5.3.1. Accuracy (IPP 9 [PPIP s16] and HPP 9)

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.

We ensure the accuracy of the information by collecting it directly from customers and/or employees wherever practicable, or otherwise in accordance with legislation (as set out in 4.2.4 above).

5.3.2. Limited use (IPP 10 [PPIP s17] and HPP 10)

We may use personal and health information:

- *for the primary purpose for which it was collected*
- *for a directly related secondary purpose*
- *another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health*
- *another purpose for which the person has consented*
- *another purpose where permitted by law.*

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

Generally, we only use personal and health information for the purpose for which it was collected. The purpose should be set out in the privacy notice at the time of collection.

A directly related secondary purpose is a purpose that is very closely related to the primary purpose for collection and would closely align with peoples' 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.

Other examples of secondary purpose include:

- quality assurance activities such as monitoring, evaluating, and auditing
- work health and safety laws require that we use information to ensure the safety of our employees
- unsatisfactory professional conduct or breach of discipline

- the information relates to a person's suitability for appointment or employment as a public sector official
- finding a missing person.

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.

5.4. Disclosure

5.4.1. Disclosure (IPP11 &12 and HPP11 &14)

We may disclose personal information if:

- The disclosure is directly related to the purpose for which the information was collected, and we have no reason to believe that the individual concerned would object to the disclosure
- The individual has been made aware in the privacy notice that information of the kind in question is usually disclosed to the recipient
- We reasonably believe that the disclosure is necessary to prevent or lesson an imminent of threat to life or health
- Where the disclosure is otherwise authorised by law.

Higher protections are afforded to sensitive personal information.

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

We can generally disclose health information when the person has consented to the disclosure; the disclosure is directly related to the purpose for which it was collected, and the individual would reasonably expect us to disclose the information for that purpose; or the disclosure is necessary to prevent or lesson a serious or imminent threat to life, health or safety.

It is important to note that 'disclose' is different to 'use'.

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

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.

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 PPIPA and HRIPA 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.

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, including:

- 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
- 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.

5.4.2. Identifiers (HPP 12)

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

Identifiers are used to uniquely identify an individual and their health records. An identifier does not need to use a person's name as they are designed to be unique to a specific individual (for example, a customer number, unique patient number, tax file number or drivers licence number).

5.4.3. Anonymity (HPP 13)

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

This HPP is not relevant to our functions and activities.

5.4.4. Linkage of health records (HPP 15)

We only use health records linkage systems if an individual has provided or expressed the consent, unless the linkage is for research purposes and has been approved in accordance with statutory guidelines.

We will only use health record linkage systems when individuals have expressly consented to their information being included on such a system, or for research purposes which have been approved by an Ethics Committee and in accordance with Statutory Guidelines on Research.

5.5. Exemptions on how we manage personal and health information

5.5.1. When the principles do not apply (IPPs and HPPs)

The IPPs and HPPs do not apply in certain situations or to certain information collected. 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 limited circumstances
- 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.

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 PPIPA contains exemptions that may allow DCS 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 non-compliance is otherwise permitted or is necessarily implied or reasonably contemplated under an Act or law. For example, if information is shared, 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 agencies concerned, for example, for the use of corporate services of another agency

5.6. Information published on public registers (Part 6 of PPIPA)

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 listed on the NSW Fair Trading website 'public register' page or the OneGov (Service NSW) website 'public register' page

These lists are not exhaustive. However, if you would like to confirm public register information directly with an agency, please contact the employee or business area dealing with the information or as outlined in the 'contact us' section.

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 email: 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.

5.7. The Australian Criminal Intelligence Commission

Where necessary, DCS also requests police checks from 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.

5.8. Statistical information

We will use anonymised, 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.

6. 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 or expense. We do not charge any fees to access or amend personal or health information unless you are lodging a formal application under the *Government Information (Public Access) Act 2009* (GIPA Act).

6.1. Informal requests

An informal request means that you contact the relevant division, agency or business unit within DCS and ask for the information you are seeking. There are no fees required and no formal requirements to be met, such as a form, before your request will be actioned.

You can contact the relevant division, agency or business unit within DCS directly. You can also contact the relevant Privacy Lead or email: privacy@customerservice.nsw.gov.au.

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

6.2. Formal requests

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

No fee is required if you are requesting information under the PPIPA HRIPA, but there is a fee if your request is made under the GIPA Act.

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

The Office of the Privacy Commissioner, within the Information and Privacy Commission (IPC), can also provide help and guidance about your rights around your personal and health information (refer to the ‘contacts’ tab for information for how to contact the IPC).

6.3. 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 PPIPA and HRIPA give you the right to access your own information, the Acts generally does not give you the right to access someone else’s information.

However, both PPIPA and HRIPA 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 years of age, we are allowed to collect information directly from your parent/s or guardian.

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

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

7. Your Review and Complaint Rights

DCS encourages you to contact us directly to resolve any concerns you have about our handling of your personal and health information.

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 employees member or the division, agency or business unit dealing with your information (if known).

7.1. Informally

We encourage people to try to resolve privacy issues with us informally before going through a review process. We recommend that the individual contact us by email at privacy@customerservice.nsw.gov.au.

The DCS Privacy Officer:

- Responds to enquiries about how we manage personal and health information
- Responds to requests for access to and amendment of personal and health information
- Provides guidance on broad privacy issues and compliance
- Conducts internal reviews about possible breaches of PPIPA and HRIPA (unless the subject of the review is the conduct of the Privacy Contact Officer).

The request does not need to be in writing, but a formal application may be required.

If a person is unhappy with the outcome of their informal request, they can still make a formal application for internal review. However, by law, you have only six 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.

7.2. Your Right of Internal Review

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

By law, an application form for internal review must:

- Be in writing
- Be addressed to DCS (you may also specify the business area within DCS to which the complaint relates, if relevant), and
- include a return address in Australia to which you can be notified after the completion of the review.

To help you apply for an internal review, you can use the application form from the IPC. This can be downloaded from the IPC website https://www.ipc.nsw.gov.au/privacy/citizens/make-complaint-forms. Although we encourage you to use the form, you don't have to. You may submit any other relevant material along with your application.

You do not have to make specific reference to the privacy legislation in an application for internal review. However, an application must, on the face, reasonably convey to DCS that an application for internal review is sought. The absence of any reference to the privacy legislation, information protection principles or the concept of privacy may indicate to DCS that a complaint is an expression of grievance and request for action rather than an application for internal review.

If you are helping someone who can't read or write in English and/or their first language to make an application, and an organisation isn't making the application on their behalf, the DCS GIPA and Privacy Team will use a professional interpreter to help you to make your application.

7.2.1. Process

Under privacy law, an internal review must be undertaken by the agency concerned. This means that DCS will undertake the internal review.

The person conducting the internal review will examine relevant material and may make inquiries with other people within DCS. The person conducting the review may contact you to clarify the scope of your application.

As far as possible, the internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is a member of the DCS Privacy Team, or another person who is an employee or an officer of DCS, and
- is qualified to deal with the subject matter of the complaint.

Internal reviews follow the process set out in the Information & Privacy Commission's Internal Review Checklist.

When the internal review is completed, the applicant will be notified in writing of the:

- findings of the review
- reasons for those findings
- action DCS proposes to take
- reasons for the proposed action (or no action)
- applicant's entitlement to have the findings and the reasons for the findings reviewed by NSW Civil and Administrative Tribunal (NCAT).

We are required to give a copy of your internal review request to the Privacy Commissioner, in addition to a copy of the draft internal review report. We must consider any submissions made by the Privacy Commissioner and we will keep the commissioner informed of the progress of the internal review. We will also provide the commissioner with a copy of the finalised internal review report.

For further information about the internal review process, contact us by email at privacy@customerservice.nsw.gov.au

You cannot make an application to DCS about the conduct of another "public sector agency", including other public sector agencies within the DCS cluster. If the conduct you are concerned about is by another agency, you will need to make your application to that agency. The DCS Privacy Team is able to provide general privacy advice and assistance to other agencies within the cluster but cannot conduct internal reviews for them.

7.2.2. Timeframes

You must lodge your request for internal review within six months from the time you first became aware of the conduct that you think breached your privacy.

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

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

- Complete the internal review within 60 calendar days
- Respond to you in writing within 14 calendar days of completing the internal review.

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

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

7.3. Your Right of External Review

You have the right to apply to the NSW Civil and Administrative Tribunal if you have sought an internal review and you are not satisfied with the:

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

For more information about seeking an external review, refer to section 9.3 below for the Tribunal's contact details.

7.4. Complaints to the Privacy Commissioner

You have the option to complain directly to the Privacy Commissioner if you believe that we have breached your privacy. Refer to section 9.2 below for the Privacy Commissioner's contact details.

8. Strategies for Compliance and Continuous Improvement

DCS is committed to protecting the privacy rights of customers, employees and members of the public.

We adopt several strategies to implement best practice principles and comply with our obligations under PPIPA and HRIPA that recognises that privacy is a shared responsibility within the cluster.

8.1. Policies and procedures

We have developed policies, standards and guidelines to inform and assist employees in protecting privacy. These policies provide best practice guidance and practical advice on matters relating to:

- Acceptable use of technology
- Dealing with confidential information
- Information security
- Records management
- Privacy breaches
- Use of social media

Our Code of Ethics and Conduct outlines the responsibilities of our employees in protecting privacy in the course of their duties. All employees are provided with a copy of the Code and are regularly reminded of their obligations.

We consistently review and update our policies and procedures when necessary.

Policies and procedures, including this DCS PMP, are communicated to employees in a range of ways, including through our intranet, printed copies and targeted on-the-job training. Information about our privacy practices is also made available on our dedicated privacy intranet page.

8.2. Promoting privacy awareness

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

8.3. Review and continuous improvement

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

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

A cluster-wide Privacy Partners Network forum is held that comprises of representatives from all DCS divisions and agencies. The forum meets regularly to discuss privacy and identify opportunities for better practice in protecting privacy.

8.4. Directions of the Privacy Commissioner to modify PPIPA or HRIPA

The Privacy Commissioner may make a direction to waive or modify the requirements for a public sector agency to comply with an IPP or HPP or a privacy code of practice.

Agencies can request a direction. The general intent is for the directions to apply temporarily. If a modification is required for longer, then a privacy code of practice may be more appropriate.

A privacy code of practice may be created to allow an agency to modify the application of one or more IPPs or HPPs or specify how they are to be applied to particular activities or classes of information.

8.5. When can information be shared with others for analysis

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) was created to promote sharing of information for certain purposes which include allowing the government to carry out data analytics for the purposes of identifying issues and solutions to better develop government policy, program management, and service planning and delivery. The DSGS Act provides for the expeditious sharing of information with the Data Analytics Centre (DAC) or between other government sector agencies. It also provides protections in connection with data sharing and ensures compliance with the requirements of PPIPA and HRIPA.

Before responding to a request from the DAC to provide information, we may ask the Privacy Commissioner to guide us on the best way to comply with the request. Other agencies, such as NSW Police, the Ombudsman's Office, ICAC may send us a request for information. When such a request is received, we ask for it in writing, to include the relevant legislation that allows for the sharing of information, and for the request to nominate a contact person.

Before releasing information to the other agency, we check the named legislation and ensure the request is legitimate. This is often done by contacting the nominated officer by telephone, using the generic number for the agency.

8.6. When should a Privacy Threshold Assessment and Privacy Impact Assessment be done?

A Privacy Threshold Assessment (PTA) is a preliminary assessment to help determine a project's potential privacy impacts and the risk level, including whether it could be a 'high privacy risk project'. It considers what privacy obligations may apply to an activity, project or proposal. Depending on what is proposed in the PTA you may require a subsequent Privacy Impact Assessment (PIA) to be completed for your project. A PTA should be performed if the project involves new or changed ways of handling personal information.

A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. It may be required to assess any actual or potential effects that an activity, project or proposal may have on personal information. A PIA can also outline ways in which any identified risks can be mitigated, and any positive impacts enhanced. It may not be possible to eliminate or mitigate every risk, but ultimately a judgement will be made as to whether the public benefit to be derived from the project will outweigh the risk posed to privacy.

To know if a PIA is required, employees assess whether the project involves any change to how personal information is sighted, collected, linked, analysed, used, disclosed, accessed, secured, stored, retained, transferred, or how individuals are viewed, tracked or monitored. If

there is any change, then the DCS Privacy Team advise employees on whether a PIA is necessary.

8.7. Notification of a Data Breach

If a data breach is identified, whether serious or not, affected individuals will be notified wherever possible, unless notification poses greater harm to the affected individuals, or the information breached is not sensitive and poses little to no risk of harm to the affected individuals.

Notifying individuals can assist in mitigating any damage for those people and reflects positively on our organisation. If the data breach creates a real risk of harm to the individual, then they must be notified immediately, or as soon as possible.

The NSW Privacy Commissioner is notified of any privacy/data breach.

9. Key Contacts

9.1. DCS Privacy Team

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

Email: privacy@customerservice.nsw.gov.au

Web: www.customerservice.nsw.gov.au

Mail: Level 22, McKell Building, 2-24 Rawson Pl, Sydney NSW 2000

Visit: Documents, enquiries or complaints can be lodged via any Service NSW centre. The Service NSW centre locator can be found at: https://www.service.nsw.gov.au/service-centre or by ringing Service NSW on 13 77 88.

9.2. The NSW Information and Privacy Commission (IPC)

The NSW Privacy Commissioner's contact details are:

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Web: www.ipc.nsw.gov.au

Post: PO Box R232 Royal Exchange NSW 2001

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

9.3. The NSW Civil and Administrative Tribunal (NCAT)

NCAT's contact details are:

Phone: 1300 006 228

Fax: 02 8114 3756

Web: www.ncat.nsw.gov.au

Post: NSW Civil & Administrative Tribunal, Administrative and Equal Opportunity Division, GPO Box 4005, Sydney NSW 2000.

9.4. Relevant Agency Privacy Lead Contacts

Privacy Leads within specific DCS agencies or divisions covered by this DCS PMP regarding personal information known to be held by the specific agency or division.

Division/ Agency	Contact details
Births, Deaths and Marriages	Email: bdm-complaints@customerservice.nsw.gov.au
Better Regulation Division	Email: BRDPrivacy@customerservice.nsw.gov.au Phone 02 9219 3999
Hardship Review Board	Email: RNSWprivacy@revenue.nsw.gov.au
Long Service Corporation (LSC)	Web form: https://www.longservice.nsw.gov.au/contact-us/feedback
Revenue NSW	Email: RNSWprivacy@revenue.nsw.gov.au
Safework NSW	Email: privacy@safework.nsw.gov.au Phone: 13 10 50

Privacy Officers within specific DCS agencies NOT covered by this DCS PMP for personal information held by that agency.

Agency	Contact details
Independent Pricing and Regulatory Tribunal (IPART)	Email: ipart@ipart.nsw.gov.au Phone: (02) 9290 8400
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 Independent Review Officer (IRO)	Email: complaints@iro.nsw.gov.au Phone: 13 94 76
Personal Injury Commission (PIC)	Email: privacy@pi.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

Otherwise, contact the DCS Privacy Team by email at:
privacy@customerservice.nsw.gov.au to help direct your request, or questions.

10. Resources – Other Related Laws

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

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

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

For more information on the operation of the GIPA Act and your personal information, please contact our DCS GIPA team via the DCS website.

General Data Protection Regulation (GDPR)

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

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

Under this law the Information Commissioner has the power to access government information held by other NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint under the GIPA Act and Government Information (Information Commissioner Act – GIIC). The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

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

For further information on the operation of the GIIC Act, contact the IPC (refer to the 'contacts' tab for information for how to contact the IPC).

Privacy Act 1988 (Privacy Act)

Under the Privacy Act, the Australian Information Commissioner has a number of 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).

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

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

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

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

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

11. Glossary of Terms

Agency	A 'public sector agency', as defined in section 3 of the PPIPA.
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 agency	DCS or any other agency within the cluster
Collection (of personal information)	The way information is acquired by DCS. This can include a written form, a verbal conversation, an online form or a photographic image
DCS or Department of Customer Service	Refers to the Department of Customer Service.
Disclosure (of personal information)	Means providing personal information to an individual or entity outside of DCS, including to another cluster agency.
Health information	Personal information or an opinion about a person's physical or mental health or disability, or a person's express wishes about future provision of health services or a health service provided, or to be provided to a person. Any personal information collected for the purposes of the provision of health care will generally be 'health information' and will also include personal information that is not itself health-related but is collected in conjunction with health service provision.

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* (PPIPA). 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
Investigative agency	Any of the following: the NSW Ombudsman Office, the Independent Commission against Corruption (ICAC) or the ICAC Inspector, the Police Integrity Commission (PIC) or the PIC Inspector, the Health Care Complaints commission, the Office of the Legal Services Commissioner.
Law enforcement agency	The NSW Police Force, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the Director of Public Prosecutions, Department of Corrective Services, Department of Juvenile Justice, Office of the Sheriff of NSW.
Personal information	Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes such things as individual's fingerprints, retina prints, body samples or genetic characteristics. Exclusions to the definition of personal information are contained in s4(3) of the PPIPA. Health information is like a special type of personal information and is regulated separately.
Public register	A register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee).

Public sector agency	A 'public sector agency', as defined in section 3 of PPIPA. 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.
Privacy Code of Practice	This is a document approved by the NSW Privacy Commissioner that provides for specific exemptions from the Information Protection Principles to carry out their functions. See for example the NSW Fair Trading Privacy Code of Practice.
Privacy obligations	The information privacy principles and any exemptions to those principles that apply to DCS
Sensitive information	Means information referred to in section 19(1) of PPIPA. 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.
Employees	Any person working in a casual, temporary or permanent capacity in DCS, including volunteers, consultants, contractors and any person performing a public official function whose conduct could be investigated by an investigating authority.

12. Document Control

12.1. Document Approval

Name & Position	Date
Andrew Pilbeam, Director, Governance, Governance Risk and Performance, Corporate Services	31 May 2022
Belinda Lawn, Executive Director, Governance Risk and Performance, Corporate Services	14 June 2022
Mandy Young, A/ Chief Operating Officer (A/ Deputy Secretary, Corporate Services)	14 June 2022

12.2. Document Version Control

Version	Status	Date	Prepared By	Comments
1.0	Draft	22 March 2021	Andrew Pilbeam	Draft for Consultation
2.0	Draft	31 March 2021	Andrew Pilbeam	Revisions. Draft for Approval
2.0	Approved	31 March 2021	Andrew Pilbeam	V2.0 Approved by: ED GRP DCS COO
2.1	Review	28 May 2021	Katarina Cvitkovic	Privacy Uplift review
	Review	June 2021	Privacy Partners Network / Legal / Other	For consultation
2.2	Collation of feedback	July 2021	Katarina Cvitkovic	Review/Update
2.3	Review	August 2021	Privacy Partners Network	2nd consultation
	Collation of feedback	September 2021	Katarina Cvitkovic	Review/Update
	Review	April 2022	Andrew Pilbeam	Review/ Update Machinery of Government
2.4	Approved	June 2022	Andrew Pilbeam	V2.4 Approved
2.5	Approved	August 2022	Andrew Pilbeam	Update to include LSC in this plan