Privacy Management Plan 2020
Department of Communities and Justice

Version date: 18 August 2020

Table of Contents

Introduction

Purpose

This Privacy Management Plan explains how the Department of Communities and Justice (the Department) complies with obligations under the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act). More information about the PPIP Act and the HRIP Act is accessible from the Information and Privacy Commission at www.ipc.nsw.gov.au

This plan sets out the Department's commitment to respecting the privacy rights of our employees and contractors, the people we provide services and support to, as well as their families and carers, and other people whose information we hold. This plan is produced in accordance with the requirement for a Privacy Management Plan under section 33 of the PPIP Act and demonstrates how the Department ensures compliance with the PPIP Act and HRIP Act. The plan explains how we manage personal information in line with the PPIP Act and health information in line with the HRIP Act. It identifies who a person can contact with questions about the personal or health information we hold, how information can be accessed or amended and what to do if there is a concern about a breach of the PPIP Act or HRIP Act. We also use this plan to train our employees about dealing correctly and lawfully with personal and health information to promote compliance with the PPIP Act and the HRIP Act.

The 2020 plan updates references and structural changes in our Department since 1 July 2019 following machinery of Government changes. Our organisational chart is available through the following link: https://www.dcj.nsw.gov.au/about-us/building-stronger-communities.html

The first half of this plan covers how the Department generally collects and handles personal information. To see how each Division handles personal information **specific to that Division**, so far as it differs from the general approach, please click here.

The PPIP Act and the HRIP Act contain criminal offence provisions applicable to our employees if they access, use or disclose personal information or health information without authorisation. We use a broad range of electronic databases to hold the information we collect, and if an employee accesses, uses or discloses personal or health information for their own personal purposes they may be subject to prosecution and/or disciplinary action. There are also offences in the *Crimes Act 1900* for using a computer to access information without authority. Fact sheets outlining some of the more common record types of information we hold is available here.

Employee access to client databases such as OIMS (the Offender Integrated Management System), ChildStory, HOMES, EDRMS/One TRIM is strictly for authorised work purposes only.

What this plan covers

Section 33(2) of the PPIP Act sets out the requirements of this plan. This plan must include:

- information about how we develop policies and practices in line with the PPIP Act and the HRIP Act
- how we train employees in these policies and practices
- our internal review procedures
- anything else that we consider relevant to the plan in relation to privacy and the personal and health information we hold.

This plan covers the Department of Communities and Justice and its Divisions. There are several aspects of compliance with privacy obligations common to all Divisions as set out in the first part of this plan.

While we try to ensure consistency across the Divisions in how personal information is handled, each Division differs in its functions and activities. Further details regarding the differences that exist between Divisions can be accessed by clicking on relevant links in this plan.

When we review this plan

We will review this plan every 12 months. We will review the plan earlier if any legislative, administrative or systemic changes impact on our management of personal and health information.

Mandatory Requirements

All employees are required to comply with the PPIP Act and the HRIP Act. This plan is designed to assist employees to understand and comply with their obligations under the PPIP Act and the HRIP Act. It is also intended to provide the community with information about how we meet our privacy obligations.

Advice and support for employees is available from the Open Government, Information and Privacy Unit, Legal (infoandprivacy@dcj.nsw.gov.au) in relation to privacy compliance, rights and obligations.

Implementation

The Department's employees are responsible for:

- familiarising themselves with and complying with the Privacy Management Plan when dealing with personal and health information,

- identifying whether new projects are likely to raise privacy issues and consulting Legal (infoandprivacy@dcj.nsw.gov.au) where appropriate,
- identifying and raising privacy concerns with their Manager or Director, and Legal as appropriate, and
- participating in privacy training to improve their knowledge and awareness of privacy obligations.

Promoting privacy awareness

We take our privacy obligations very seriously and undertake a range of initiatives to ensure our employees, contractors and members of the public are informed of our privacy practices and obligations under the PPIP Act and the HRIP Act. We promote privacy awareness and compliance by:

- publishing and promoting this plan on our intranet and website,
- incorporating privacy information in our induction program and in the modules for Code of Conduct and Fraud and Corruption awareness,
- publishing and promoting all privacy policies on our intranet,
- maintaining a dedicated privacy page on our intranet that centralises all privacy resources for our employees and that provides information about what to do if employees are unsure about a privacy issue,
- drafting and publishing privacy factsheets on our intranet to provide employees with practical guidance on privacy issues and considerations,
- delivering periodic face to face and online training across different business areas,
- providing a dedicated privacy advisory service to employees,
- investigating allegations of breaches of privacy and implementing recommendations made from finalised investigations,
- assessing privacy impacts of new projects or processes from the outset,
- working with senior executives endorsing a culture of good privacy practice,
- educating the public about their privacy rights and our obligations (for example, maintaining a dedicated privacy page on our website and providing privacy information on forms that collect personal and health information).

Who we are

The Stronger Communities Cluster was created on 1 July 2019, bringing together and replacing the Family and Community and Justice Clusters. This brings under one roof, NSW government services targeted at achieving safe, just, inclusive and resilient communities. This plan relates to the information handling practices of the Department, as the lead agency in the Stronger Communities Cluster. The Department delivers a range of services, including but not limited to the following:

- child protection services (early intervention and preservation, statutory child protection and out-of-home-care)
- community inclusion services (carers, ageing, disability inclusion)
- assistance with housing and homelessness

- legal, court and supervision services to the people of NSW by managing courts and justice services
- implementing programs to reduce crime and re-offending
- managing custodial and community-based correctional services, protecting rights and community standards
- advising on law reform and legal matters.

A number of Privacy Codes of Practice (Codes) and Public Interest Directions (PID) vary the operation and application of the PPIP Act and the HRIP Act to enable some of our functions. These Codes and PIDs are Agency or Division specific in their operation. The Codes and PIDs enable us to provide services in line with the Premier's Priorities including domestic violence intervention, reducing offending recidivism and protecting our most vulnerable children. The applicable Codes and PIDs are discussed in greater detail in this Privacy Management Plan and the Business Units that have responsibility for delivering these outcomes. This plan will be amended as new Codes and / or PIDs are approved by the Privacy Commissioner, Attorney General and / or Health Minister.

For further information about our Department, its structure and each Division, click here.

Application of this plan

The PPIP Act is concerned with 'personal information'. Personal information is defined in the PPIP Act as being "any information or opinion about a person whose identity is apparent or can be reasonably ascertained from the information or opinion."

While the definition of 'personal information' is very broad, there are some important exceptions to the definition. The exceptions that are most relevant to the Department is information:

- arising out of a Royal Commission or Special Commission of Inquiry
- contained in Cabinet documents
- about an individual's suitability for appointment or employment as a public sector official
- arising from the exercise of specific statutory law enforcement powers such as telephone interception, controlled operations and witness protection.

These exceptions do not interfere with the confidentiality or sensitivity of these types of information and exemptions from the requirements of the PPIP Act does not mean that other policy or statutory requirements, such as the confidentiality of Cabinet documents, can be disregarded.

The information protection principles cover the full potential 'life cycle' of information, from the point of collection through to access, use, disclosure and archiving and/or the point of disposal. They include obligations with respect to data security, data quality (accuracy) and rights of access and amendment to personal information, as well as how personal information may be collected, used and disclosed.

Main classes of information collected by the Department

We hold a range of information, including information that falls within the definition of 'personal information' under the PPIP Act and some 'health information' as defined in the HRIP Act.

Further information on the Health Privacy Principles (HPPs) and the Information Protection Principles (IPPs) is available through the following links:

The Health Privacy Principles (HPPs)

The Information Protection Principles (IPPs)

Given the broad range of functions and activities covered by our Divisions a general description of information commonly held by our agencies is captured below. These include:

- personnel records (the Public Sector Personnel Handbook gives detailed directions on handling employee records – including limited records of contractors)
- administrative records (most of this information is collected automatically as a result of people using a particular service, for example, vehicles, telephone, email)
- correspondence
- submissions and consultation responses
- child protection and out of home care records as well as Youth Justice records
- custodial records
- adoption records
- information of clients receiving housing assistance products (such as Bond Loans), the NSW Housing Register and public housing tenancy information
- complaint files (agencies that handle complaints generally have in place standard complaints handling procedures that provide further detail)
- case files (courts and tribunal's case files that relate to the exercise of judicial functions, are exempt from the operation of the Information Protection Principles).
- legal files that include legal advice, client instructions, information relevant to hearings, etc.

Information collected by agencies that is unique to those agencies is broadly described in this plan.

The Department as a Law Enforcement / Investigative Agency

The Department of Communities and Justice is considered a law enforcement agency for the purposes of the PPIP Act. This means in carrying out some of our functions and activities we are not required to comply with some of the information protection principles in the PPIP Act regarding the collection, notice, use and disclosure of personal information in particular contexts.

We are also an investigative agency for the purposes of the PPIP Act when we exercise some of our functions under the authority of an Act and those functions may result in disciplinary, criminal or other formal action. For example, when exercising our investigative functions under the *Residential Tenancies Act 2010* we are not required to comply with some of the information protection principles in the PPIP Act, including how we collect, use and disclose personal information.

Contracted service providers

We are responsible for protecting personal information handled on our behalf. Where it is necessary for personal information to be transferred to a third-party provider for the purposes of providing services to our clients or to us, we develop and execute contract terms that prevent them from unauthorised use or disclosure of personal information that we hold. This includes community housing providers participating in Housing Pathways, the Aboriginal Housing Office (AHO) and the Land and Housing Corporation (LAHC).

The Department of Communities and Justice

We may also use your information from various Divisions in the Department, to plan, coordinate and improve the way we provide services. Divisions may, where permitted under the PPIP Act or a relevant Privacy Codes of Practice or Public Interest Directions, exchange information with other Divisions in the Department to provide a single view of a client, conduct research and analytics of data or otherwise better coordinate, plan and deliver services to members of the public.

Collection (PPIP Act section 8-11, HRIP Act HPP 1-4)

Personal information and health information must only be collected by lawful means for purposes related to our functions and activities. Wherever possible we must collect personal information and health information directly from the individual to whom the information relates. The collection of personal information and health information must not unreasonably intrude into the personal affairs of the individual.

The Department takes active measures to ensure that the collection of personal and health information is relevant, not excessive and is not an unreasonable intrusion into the affairs of an individual by encouraging business units to regularly review

privacy collection notices to ensure they accurately reflect the collection of personal information relevant for business needs, review and update Department's Privacy Policy and provide regular on-line / face-to-face privacy training.

Generally, when we collect personal and health information, the information is collected directly from the individual. However, the individual may authorise the collection of their information from another person. Given the breadth of the functions and activities of our divisions, the collection of information by each Division is broadly set out here.

When collecting personal and health information from individuals, we give a privacy notice to the individual to whom the information relates. Section 10 of the PPIP Act and schedule 1 Clause 4(1) of the HRIP Act sets out what is required in this notification. This includes the purpose for collection, intended use and recipients, whether the information is required and the individual's right and method of access and amendment to that information. Where health information is collected from someone other than the individual, the individual will be notified as soon as possible after the collection unless an exemption or exception applies.

As noted above we are a law enforcement agency as defined in section 3 of the PPIP Act. As part of our law enforcement functions, we facilitate and administer several crime prevention and crime intervention programs. In certain circumstances, we may collect information other than directly from the individual. We may also use information for a purpose other than the purpose for which the information was collected without the express consent of the individual for law enforcement purposes. This additional collection and use will only be conducted in accordance with the exemptions under Division 3 of the PPIP Act or as provided for by an approved and gazetted Privacy Code of Practice or Public Interest Direction.

Personal information collected during enquiries

Personal or health information collected during our enquires is collected to accurately record the management of the matter and is required to be collected, used and stored in compliance with the PPIP Act and HRIP Act.

Each of our Divisions receive many different types of enquiries. Enquiries are received by phone, email, in writing and in person. People may provide names, contact details, opinions, health conditions and illnesses, family relationships, work history, education and criminal history. The personal information and health information collected by each Division and agency to enable an appropriate response to the enquiry will vary depending on the nature of the enquiry. Specific information about the collection of personal information and health information relevant to each agency can be obtained by contacting the agency directly and / or reviewing the agency's website or forms/notices for collection.

Employee records

For various reasons, such as leave management, workplace health and safety and operational requirements, we must keep employee records including:

- documents related to the recruitment process
- payroll, attendance and leave records
- banking details and tax file numbers
- training records
- worker's compensation records
- workplace health and safety records
- records of gender, ethnicity and disability of employees for equal opportunity reporting purposes
- medical conditions and illnesses
- next of kin and emergency contact
- secondary employment
- conflicts of interests.

This information is collected directly from employees and will be managed in accordance with the provisions of the PPIP Act and the HRIP Act. We maintain business records that contain personal information including contact details for public officials in other government entities, as well as other third-party organisations. Health information may also be collected and retained consistent with our obligations under the HRIP Act and Contracts with other government and third-party entities and individuals may include personal information or health information but is only collected in accordance with the privacy principles. This may include individuals engaged as contractors rather than ongoing employees.

Use (PPIP Act section 17, HRIP Act HPP 10)

We collect, use, store and disclose personal and health information of individuals for several reasons for the purpose of fulfilling our functions and activities. The terms 'use' and 'disclosure' are not defined in privacy legislation however case law has developed to give them different meanings under the Act.

In general, to 'use' information means to handle information that has been collected, and requires some administrative action or consequence for example, an employee using a person's personal information to prepare a report. To 'disclose' information means to give information collected by us to a person or body outside of our Department for example, if we were to provide information to the NSW Police Force.

When considering whether to use personal information or health information we hold, we must consider whether:

- the proposed use is consistent with the purpose for which it was collected, or
- the proposed secondary use is directly related to the purpose of collection, or

- the individual has consented for use of their personal information for that purpose, or
- it is necessary to prevent or lessen a serious and imminent threat to life or health of a person.

We can use the information for the proposed purpose if any of the above circumstances apply.

One way for us to ensure that personal or health information has been used or disclosed lawfully is by obtaining consent. For consent to be valid, it must be voluntary, informed, specific, current and given by a person who has capacity to give it. When we obtain consent, we should ask:

- Does the individual have capacity to consent?
- Is the consent voluntary?
- Is the consent informed? Relevant factors include awareness of the purpose of collection, the intended use / disclosure of the information, whether disclosures are required by law, and the consequences of giving or refusing consent.
- Is the consent specific as opposed to general, blanket or bundled? (bundled consent refers to an agency using a single request process such as one checkbox to obtain consent for a wide range of collections, uses or disclosures, without giving a person the opportunity to choose which of those collections / use / disclosure they consent to.

How information is used by various Divisions and Business Units is discussed in the section below titled *Handling of information by Division*.

Disclosure (PPIP Act section 18, HRIP Act HPP 11)

We only disclose personal or health information if one or more of the following applies:

a) at the time we collected their information, the person was given a privacy notice to inform them their personal information would or might be disclosed to the proposed recipient, or

b) 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, or

c) we have reasonable grounds to believe that disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person the information is about or another person, or

d) the person concerned has consented to the proposed disclosure, or

e) it is required for law enforcement or investigation purposes. In such instances, a valid warrant or court order (subpoena) may be required, or

f) the disclosure is required, permitted, implied or reasonably contemplated by an act or any other law, or

g) the disclosure is permitted by a Public Interest Direction or Code made by the NSW Privacy Commissioner.

In addition to the Department being defined as a law enforcement agency for the purposes of the PPIP Act, Corrective Services NSW and Youth Justice are law enforcement agencies for the purposes of the HRIP Act.

It is important to note that we have the discretion to disclose personal information and health information to other law enforcement agencies without the consent of the individual concerned when a search warrant, subpoena, summons or statutory order has been issued upon us, or when the disclosure:

- concerns proceedings for an offence or for law enforcement purposes, or
- is related to the whereabouts of a person reported as missing to the police, and the disclosure is to be made directly to a law enforcement agency, or
- is reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe that an offence has been committed.

Health information must be protected from unauthorised use and disclosure wherever it is held and any authorised uses and disclosures made of it should be tracked or recorded.

Given the breadth of our functions and activities, further information about the disclosure of information by some Divisions, is set out here.

Restricted personal information

The following categories of personal information are given more stringent protection under section 19 of the PPIP Act:

- an individual's ethnic or racial origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- sexual activities

These categories of information are only collected when required for a particular function or activity and may only be disclosed if it is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or of another person.

Exemptions apply only when providing services or assistance to specific groups, or where other legislation requires or reasonably contemplates disclosure (see section 25 of the PPIP Act).

Storage and Security of Personal Information (PPIP Act section 12, HRIP Act HPP 5)

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

We use a variety of information management systems to manage our storage and security obligations including paper-based filing systems, and electronic records forming part of secure computerised databases. Strict rules are followed for storing personal information and health information in all its formats in order to protect personal information and health information from unauthorised access, loss or other misuse. Only those employees who need to know particular personal information or health information in order to carry out their work can have access to it.

Personal information and health information, both paper-based and electronic media, must be stored securely in our electronic systems and protected from unauthorised access and alteration. Personal information and health information must be kept only as long as it is necessary for the purposes for which it may lawfully be used. When it is no longer needed, the personal information or health information must be destroyed using a secure waste destruction service (for paper-based documents) and formal deletion processes for electronic documents and data.

Personal and health information held in our records can only be disposed of in accordance with the *NSW State Records Act 1998* and the relevant disposal authorities. This link provides a list of relevant Functional Disposal Authorities. A list of the specific storage, security and disposal authorities for some divisions is set out by division here. To view other specific authorities please follow the previous link.

The information we hold and the communication of this information internally and externally is subject to our security policies. This is available for employees on the intranet. If you would like a copy of a particular policy, guideline or procedure, please contact information.security@dcj.nsw.gov.au to request a copy.

Where it is necessary for personal or health information to be transferred to a person in connection with the provision of a service to us, we will take steps to prevent unauthorised use and disclosure of that information. We comply with our obligations by reviewing contracts to ensure that privacy obligations are imposed on contracted service providers and that they comply with the Information Protection Principles and the Health Privacy Principles.

We require data breaches to be promptly notified to the Open Government, Information and Privacy Unit, Legal and to Information and Digital Services by our employees and by contracted service providers. This ensures a co-ordinated approach when it comes to managing any reported incident. This includes determining whether it is appropriate to report a data breach to the NSW Privacy

Commissioner or the Federal Privacy Commissioner, as well as providing advice and assistance to aggrieved individuals and implementing measures to address any systemic issues.

Data Breaches

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* establishes a Notifiable Data Breaches scheme (NDB). NDB applies to the Department as a tax file number (TFN) recipient as we hold TFN's for employment and other business related purposes. A TFN recipient is any person who is in possession or control of a record that contains TFN information.

A NDB is a data breach that is likely to result in serious harm to any person to whom the information relates. A data breach may occur where personal information held by us is lost or subject to unauthorised access or disclosure.

Further information about the NDB scheme is available here from the Office of the Australian Information Commissioner.

A data breach or allegation of a breach (regardless of whether it is captured by the NDB scheme or not) must be promptly notified to the Open Government, Information and Privacy Unit, Legal.

Legal will provide advice and guidance to the relevant business unit where the breach occurred to enable the business unit to effectively deal with the incident/alleged breach. The business unit will be responsible for responding to a data breach notification which may include conducting targeted inquiries about the nature and extent of the breach, notification of affected individuals, determining whether to notify the NSW Privacy Commissioner/ Commonwealth Privacy Commissioner, preparing appropriate briefings to the relevant Deputy Secretary / Secretary and facilitating remedial action.

Access and Amendment (PPIP Act section 14 -15, HRIP Act HPP 7-8)

The PPIP Act and the HRIP Act both establish a right of access to information for individuals about themselves.

Individuals are entitled to know whether information about them is held by us, the nature of the information, the main purposes for which it is used, and how they can gain access to it, including a right of correction if details are not correct.

Informal Requests

A person wanting to access or amend their own personal or health information can make a request by contacting the relevant business unit that manages their information. Generally, this request does not need to be made in writing, however a written request may be required to ensure the request is accurately understood and actioned. If a person is not satisfied with the outcome of their informal request, they

can make a formal application. If the business unit is uncertain about providing access to personal information sought by an individual, advice can be sought from the Open Government, Information and Privacy Unit, Legal..

Formal Application

A person can make a formal application for access to personal information under the HRIP Act or the PPIP Act by requesting it directly from the relevant business area in writing or by seeking advice about how to do this by contacting us at infoandprivacy@dcj.nsw.gov.au

The Department will aim to respond to the formal application in 30 working days, depending on the volume of information requested, and will advise the applicant approximately how long the application will take to process, particularly if it may take longer than expected.

Most records held about an employee are on their 'P File', which is managed by the Business Support Centre (BSC). To access their file, employees can log a ticket for the BSC through the 'Service Now' portal available on the Intranet.

Limits and reasons for refusal

We do not charge for providing access to personal information, but reasonable fees may be charged for providing access to health information.

Where an application to access information held by us includes the personal information about another person, an access application should be made under the *Government Information (Public Access) Act 2009 (GIPA Act).* Further information about GIPA is available from the Department's access to information webpage.

If the person lacks capacity to apply for information, their guardian or their 'personal information custodian' may act on their behalf in requesting access.

Access to information held by a contracted service provider

If access is sought to personal or health information held by a contracted service provider that is providing a service on behalf of the Department, you may access your personal information directly from the contracted service provider. If you experience any difficulties obtaining access to your personal or health information held by a contracted service provider, please contact the Department at infoandprivacy@dcj.nsw.gov.au

If you are concerned about the time being taken for us to handle your request or concerned that one of our contracted service providers is taking too long to deal with the request, you may contact us and request an update and time frame for the matter to be dealt with. If you remain dissatisfied, there is a right to seek an internal review by contacting the Open Government, Information and Privacy Unit at

infoandprivacy@dcj.nsw.gov.au or you may complain directly to the NSW Privacy Commissioner.

Amendment or Correction of personal information

An individual can make a request to amend their personal information. A request to amend personal information held by us will be dealt within a reasonable timeframe which is generally 30 working days of receipt of the request.

An amendment application can be made verbally or in writing to the relevant business unit that holds the information or by emailing the Department at infoandprivacy@dcj.nsw.gov.au and detailing the nature of the records and the specific request for amendment.

A request for amendment may be subject to the obligations imposed on the Department by other legislation such as the *State Records Act 1998* (NSW) to keep, accurate and complete records. If there is a disagreement about whether the information should be amended, we can attach a statement from the individual to our records which provides the individual's view on the amendment.

Our employees are authorised to make appropriate amendments to general personal information (such as contact details) when a request is made. This ensures our information is accurate, relevant, up to date, complete and not misleading. Each business unit may have its own rules about making amendments to records.

Research

Various parts of the Department may collect, use and/or disclosure of personal information for research purposes in the public interest and report on such research publically in a de-identified and/or aggregate way.

Section 27B of the PPIP Act provides that the Department is not required to comply with the Information Protection Principles with respect to the collection, use or disclosure of personal information if the collection, use or disclosure of the information is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest. When doing so, the Department must take reasonable steps to de-identify the information or where the information cannot be de-identified, the information is not to be published in a publically available publication. The collection, use or disclosure of the information under section 27B of PPIP must be done in accordance with the Section 27B Statutory Guideline issued by the Privacy Commissioner.

Accuracy (PPIP Act section 16, HRIP Act HPP 9)

The PPIP Act and the HRIP Act place an obligation on the Department to take reasonable steps, depending on the circumstances to ensure that, having regard to the purpose for which personal information held by the Department is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

Generally, we collect personal information and health information directly from the individual and rely on the person providing the information to confirm its accuracy. Sometimes we will independently verify the information, if the information has been collected indirectly, for example, in conducting our child protection functions we might interview a number of individuals to understand varying perspectives. We may take steps to verify the accuracy of the information depending on the reliability of the source of the information, the lapse in time between the point of collection and any proposed use or disclosure of the information.

Health

Additional health information protection principles - Identifiers and anonymity

The HRIP Act has an additional Health Privacy Principle (HPP) (HPP 12) concerning the use of identifiers assigned by organisations to protect individuals' identities. 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 or unique patient number. Such identifiers, that have no meaning outside of the Department, should be assigned where possible in the case of provision of 'health information' for research purposes so that the data is de-identified.

Health information is defined in section 6 of the HRIP Act and broadly covers information about the physical or mental health of an individual, genetic information about an individual or a health service provided or to be provided to an individual. We take additional care when handling health information.

The NSW Privacy Commissioner has developed four statutory guidelines under the HRIP Act. They are legally binding documents that define the scope of particular exemptions in the HPPs and can be accessed here. We comply with these statutory guidelines in relation to the use and disclosure of health information.

In many circumstances, numbers are widely used to de-identify an individual. For example, Corrective Services NSW uses a (Master Index Number – MIN) to identify each inmate in custody. The use and disclosure of the identifier itself is governed by the same requirements as identified personal or health information.

Health privacy principle 13 provides the right of individuals to be given the opportunity to not identify themselves when entering into transactions with or receiving health services from us, where this is practicable and lawful. Where possible we provide individuals with the opportunity to transact anonymously or with the use of a pseudonym for example, in responding to general enquiries.

Transferrals and linkage

The Department cannot transfer health information outside New South Wales or to the Commonwealth unless we reasonably believe the receiving jurisdiction has a similar standard of privacy protection for health information. We must not include health information about any individual in a health records linkage system unless the individual has expressly consented to this.

We will only use health records 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 the Statutory Guidelines on Research

Public Registers

A public register is an official list of names, events and transactions. Under law, it is required to be available to the public. For example, we maintain the NSW Justices of the Peace Register. Information about the content of the register, how to access the information on the register and how a person can apply for their personal or health information to be suppressed in can be access by clicking on the link:

NSW Justices of the Peace (JP) Register

Privacy complaints and Internal Review

Any person can make a privacy complaint by applying for an 'internal review' of the conduct they believe breaches an IPP and/or a HPP.

A person can also discuss any concerns with the privacy team or email infoandprivacy@dcj.nsw.gov.au.

An internal review is the process by which we manage formal, written privacy complaints about how we have dealt with personal information or health information. All written complaints about privacy are considered to be an application for internal review, even if the applicant doesn't use the words 'internal review'. If you would prefer to resolve your privacy concern informally, please let us know when you contact us. We may also endeavour to deal with your complaint informally, with your consent, without the need for the formalities of an investigation.

Your rights of internal review

An application for internal review should:

- be in writing

- be addressed to the Department• specify an address in Australia at which you can be notified after the completion of the review.

To apply for an internal review, you can submit the

Privacy Internal Review Application Form in relation to a privacy breach or send your application and any relevant material by email or post to the Department.

Process

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 staff member of the Department's Legal Branch where reasonably practicable, and
- is qualified to deal with the subject matter of the complaint.

The Internal Review follows the process set out in the Information & Privacy Commission's internal review checklist. When the internal review is completed, you will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action we propose to take
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal (NCAT). We are also required to provide a copy of our draft internal review report to the Privacy Commissioner and consider any submissions made by the Privacy Commissioner.

We will keep the Privacy Commissioner informed of the progress of the internal review and will provide a copy of the finalised internal review report. Further information about the internal review process is available on the IPC website

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 will acknowledge receipt of an internal review and will aim to complete the internal review within 60 calendar days. We will contact you if the review is likely to take longer than 60 days to complete.

We will contact you in writing within 14 calendar days of completing the internal review. If the internal review is not completed within 60 days, or if you are unhappy with the outcome of the internal review you have a right to seek a review of the conduct by the NCAT.

You have 28 calendar days from the date of the internal review decision to seek an external review. To request an external review, you must apply directly to the NCAT.

To apply for an external review or to obtain more information about seeking an external review, including current forms and fees, please contact the NCAT:

Website: http://www.ncat.nsw.gov.au/

Phone:1300 006 228 or (02) 9377 5711

Visit/post: Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

Other ways to resolve privacy concerns

We welcome the opportunity to discuss any privacy issues you may have. You are encouraged to try to resolve privacy issues with an agency or business unit within the Department informally before lodging an internal review.

Complaints to the Privacy Commissioner - Individuals have the option of complaining directly to the Privacy Commissioner if you believe that we have breached your privacy. The Privacy Commissioner's contact details are:

Office: NSW Information & Privacy Commission

Level 17, 201 Elizabeth Street Sydney NSW 2000

Post: GPO Box 7011

Sydney NSW 2001

Phone: 1800 472 679 Email: ipcinfo@ipc.nsw.gov.au

Handling of information by Division

The below information details where specific Divisions handle personal and/or health information differently from the general Departmental approach outlined above or where further information about the collection, use or disclosure of personal information is relevant to the public or the Department's employees.

Courts, Tribunals and Service Delivery (CaTS)

Courts and Tribunal Services (CaTS) are responsible for the management and support of court and tribunal registries. The courts and tribunals are managed by registrars and presided over by independent judges and magistrates.

CaTS is made up of the following divisions:

- Supreme Court
- Land & Environment Court
- Industrial Relations Commission
- Local & District Courts
- Tribunals
- Court Support Services

Both personal and health information can be collected and received by courts for the purpose of determining court proceedings. Information can be held by a court in paper-based and/or digital formats.

CaTS use information held for the purposes of the Court's or Tribunal's judicial functions. Each court or tribunal is founded based on legislation and has specific legal matters over which it has authority or jurisdiction. According to section 6 of the PPIP Act, nothing in the PPIP Act affects the way a court or tribunal exercises the court, tribunal or judicial functions. Under the *Electronic Transactions Act 2000*, any information contained in an Electronic Court Management system is taken to relate to a court's judicial functions and therefore also exempt under section 6 of the PPIP Act.

Information held in paper-based format are held in secure court premises or transferred to a government records repository. Digital records can be held in various databases including the JusticeLink database (primary courts database), JudCom and Phoenix databases. Access to those databases is restricted to employees with a legitimate purpose for accessing the information held. The log-in procedure for the JusticeLink database requires officers to agree to the terms of use in accordance with our Code of Conduct each time they access the database.

Paper-based administrative records relevant to court proceedings containing personal and health information, for example, applications to postpone, waive or remit court fees, are stored separately from court proceeding documents until they no longer serve any business purpose in accordance with the General Disposal Authority GDA 28, and later securely destroyed.

Courts can also direct that certain records be sealed; those records may then only be accessed by a judicial officer or other person ordered as having permission to access. Sealed records may be retained in sealed envelopes on the court file or can be removed and held in a secure location within a court registry.

Access to digital records held by courts is provided to other government agencies that have a shared need to access information relating to court proceedings. Those agencies include:

- NSW Police Force
- NSW Bureau of Crime of Statistics and Research
- NSW Corrective Services
- Youth Justice NSW
- Office of the Director of Public Prosecutions
- Legal Aid NSW
- Roads and Maritime Services
- Revenue NSW
- Department of Communities and Justice

Access to digital information relating to court proceedings is provided to those agencies through a secure portal called Common Information Model (CIM) that each agency can subscribe to and access the information relevant to their agency's business.

Personal and health information may be provided to and received from contracted service providers for the purpose of preparing reports to courts or supporting persons attending court. These include health services and non-government organisations such as Domestic Violence Court Advocacy Services. Access to those records is managed in accordance with legislation governing access to court records.

Approved credit agencies are provided information about civil judgments as permitted by court rules. This includes personal information that identifies a person against whom a judgment has been made. This information is provided to four companies Equifax (previously known as Veda) and Illion (previously known as Dunn and Bradstreet), Experian and CreditorWatch. The operation of section 27C of the PPIP Act exempts a court agency from complying with sections 17 (use) and 18 (disclosure) of the PPIP Act relating to disclosing information to a credit reporting

body and further sets out retention periods of between 2 and 5 years for information disclosed.

The Employee Assistance Program (Benestar) and the Judicial Assistance Program (Executive Health Solutions) also hold personal and health information relating to CaTS employees.

The Office of Veterans Affairs (OVA)

The types of personal information collected and held by the OVA includes:

- photographs and film footage including that of Premier's Anzac Memorial Scholarship students, names, date of birth, occupation, marital status, residential details, telephone numbers, email addresses, social media profiles, details of parents, school and or education details, employment and or business details such as ABN's, passport information, account and banking information
- medical and health care and treatment information, risk management information for student behaviour
- service history and employment information.

The OVA generally uses and discloses personal information for the primary purpose for which it was collected. These primary purposes include:

- administering the Premier's Anzac Memorial Scholarship, and related educational initiatives
- running specific grants programs
- delivering commemorative programs delivering the Veterans employment program
- employment and personnel matters for the Department's employees and contractors

When collecting personal information OVA takes reasonable steps to ensure that the person to whom it relates is made aware of certain matters including the purpose for which it is being collected and the intended recipients of the information.

The OVA will not disclose or publish information that identifies individuals, or potentially identifies sub-groupings of addresses, without consent or otherwise in accordance with the PPIP Act.

Some circumstances where information may be disclosed, with consent, include:

- advertising for scholarships
- advertising grants program
- to Department of Education and Catholic/private schools for relevant programs
- in relation to the Veterans Employment Program

Victims Services

Personal information is collected by Victims Services from health service providers and other government and non-government agencies to identify clients, provide supporting evidence for the determination of claims, in restitution proceedings and in the investigation of Charter Complaints. A person can apply directly to Victims Services for access to their personal information, free of charge under the PPIP Act by contacting vs@dcj.nsw.gov.au.

Information is stored in Victims Services' business systems (CARES) and in hard copy files, which are stored in compactus' in secure office environments, or at the Government Records Repository. Records are currently being digitised and stored in the Department's EDRMS, accessible only by Victims Services' employees, with the ability to further enhance security for sensitive files.

Disposal is managed in accordance with the Department's disposal procedures. Hard copy files that have been scanned are destroyed via secure destruction in accordance with the *State Records Act 1998*. Information is only used for the purpose for which it was collected, that is for client identification, the determination of client claims, restitution proceeding and the investigation of alleged breaches of the Charter of Victim's Rights.

Where nominated by a client, information may be provided to third parties to assist in providing support to meet client needs. Information, including whether a person is a client of Victims Services in any capacity is treated in the strictest of confidence, at all times and is only released to those who have a right to the information. Client information may be disclosed in proceedings before courts and tribunals as directed or required by law.

Corporate Services

Corporate Services deliver services to our Department and selected cluster/independent statutory agencies with support, information and insights to achieve service delivery goals, including managing specific reforms and process initiatives projects and leading business and strategy planning. Personal information is handled by Corporate Services in line with the requirements of the PPIP Act, with the following varied requirements as to the general information protection principles under the PPIP Act.

People – Human Resources

People manage human resources including recruitment. Section 4(3) of the PPIP Act provides that information or an opinion about an individual's suitability for appointment or employment as a public sector official is not personal information for the purposes of the PPIP Act and is not subject to the Information Protection Principles.

People - Workforce Health and Safety – Injury management

Personal information is collected that is specific to the management of workers compensation injuries by the relevant Injury Management and Rehabilitation Co-ordinator (IMRC). All information is stored on corporate records systems with movement of records onto the new Work Health and Safety injury management system 'Safety Suite.'

Personal/health information can be used and disclosed for the purposes of injury management, return to work and recover at work discussions plus general claims management with all key stakeholders including injured workers and their representatives for example, the Public Service Association, an injured worker's solicitor, nominated treating doctors, service providers, insurer/claims manager, and line mangers.

Personal information is provided to the iCare appointed insurer/claims manager to assist with overall general claims management. iCare can also engage other service providers to obtain or request personal information such as independent medical examinations, factual investigations, legal referrals where an exchange of health and or personal information takes place.

All IMRCs have access to the insurer/claims manager's Case Management system/portal as 'view only' and are subject to a User Declaration confirming that access is only to be used to assist in the management of workers compensation claims. All approvals for insurer access is signed off by the Department's Workers Compensation & Injury Management Manager who explains the terms and conditions associated with same.

Strategic Finance and Procurement (SFP)

SPF manager and deliver financial services and reporting. SPF regularly access human resources related and summary data including personal information of our employees via reporting or online data produced by Enterprise Resource Planning (ER) systems. Information gathered is obtained through specific requests for the purposes of enabling employees and vendor payments to be processed, financial statements and reports to be prepared and financial analysis and audits to be undertaken, including analysis of abnormal or significant transactions. All personal information is stored within secure corporate record management systems with access restricted to authorised officers and used in-line with specific accounting standards and Treasury and Audit requirements. Information may be disclosed to the Secretary and Audit and the Risk Committee.

For procurement activities, SFP collects personal and commercial information generally through agreed data requests associated with tender information, as well as personal information of members of tender evaluation panels who are required to provide personal information to manage any conflict of interest.

Across the Department we receive **payment card data** from the public which by its nature is personal information. In processing card payments, the Department applies Payment Card Industry Data Security Standards (PCIDSS), a set of comprehensive requirements for enhancing payment account data security and forms industry best practice for any entity that stores, processes and/or transmits cardholder data.

Ministerial and Communication Services (MACS)

MACS manage all internal and external reporting and corporate communication within the Office of the Secretary and Stronger Communities Cluster Ministers' offices. External correspondence, briefing requests or requests for information received in the Office of the Secretary and Stronger Communities Cluster Ministers' offices are generally registered by MACS in the Department's electronic record management systems.

Personal information contained in correspondence or briefing requests received from the Office of the Secretary and cluster Ministers' offices may be recorded by MACS in the Department's electronic record management systems to inform responses to correspondence or briefing advice to the department and cluster Ministers. Information received from the public and the media by the MACS Media and Events team may also be stored electronically.

MACS may allocate external correspondence and briefing and information requests to specific business units to prepare Ministerial responses and/or briefing advice. Hardcopies of correspondence or requests sent to MACS are scanned and captured, along with electronic correspondence, in the department's records management systems.

MACS manages digital content on the Department's intranets and external websites. In most cases, this information is owned or provided by other business units within the Department or cluster executive agencies and every effort is made to ensure that personal and health information of individuals is not disclosed, except where consent is provided.

Information and Digital Services (IDS)

IDS deliver technology, systems and related services to the Department and independent statutory bodies supported by IDS.

IDS do not collect personal information from members of the public. IDS collect and use personal information of employees of the Department and independent statutory bodies supported by IDS which is supplied to them by the employees or others to enable IDS to provide information and digital services.

Federated Analytics Platform

The Department is in the process of implementing a Federated Analytics Platform to meet its data analytics and reporting requirements. The Platform provides a secure controlled technology platform to capture and consolidate, as required, data from a variety of internal systems, internal data warehouses, file shares, legacy stores, and external systems into one secure and managed environment.

Data collected, stored, used, disclosed and retained/disposed on the Platform is collected by the Departments agencies and business units as part of their ongoing operations. Data is also collected from third parties, such as other individuals, other NSW government agencies, non-government organisations (NGOs) providing contracted services to clients on behalf of the Department and agencies in other jurisdictions. The data includes human resources data, financial information and asset information. The data also includes personal and health information collected, used and disclosed for policy making, program and service planning, service delivery, monitoring and reporting, program and service evaluation and research.

The data includes sensitive personal information, such as information about clients' ethnic or racial background and religious beliefs. Some personal and health information is in the form of identifying unit record data, while other data is de-identified or in aggregate form. Additionally, the Department collects information relating to its client groups from data sets maintained by research bodies. Generally, this data is de-identified and/or in aggregate form.

Personal and health information may be used and disclosed on the Platform for purposes of analytics, data matching and data integration to support policy making, service planning and delivery of targeted services to meet client needs, including specifically that:

- analytics may be conducted on personal and health information to identify issues and solutions regarding policy making, program management and service planning and delivery
- analytics may be conducted on personal and health information for the purposes of determining which programs, services and types of support clients are receiving and which programs, services and support might be appropriate for them
- analytics may be conducted using information from a range of sources, such as information collected from third parties (such as other agencies with the Department, NSW government agencies, non-government service providers)
- any anticipated secondary purposes for which the data may be used (for example, that personal information may be subject to data analytics which seeks to determine the cost and effectiveness of services delivered to clients or the benefits of programs and services

Data is owned, securely stored and managed by the Department on the Platform in accordance with contractual provisions between the Department and the Platform Provider (Google Cloud Platform). These provisions include requirements to comply with privacy and record keeping laws and to store and manage information on the Platform in Australia.

Placement, storage, use, disclosure and retention/disposal of data on the Platform will be governed using the Collibra data governance tool. The tool supports management of authorisations for placement of data on the Platform, access to data on the Platform, quality of data, and use and disclosure of data on the Platform.

Corrective Services NSW (CSNSW)

CSNSW collects information to enable it to fulfil its functions and activities. A specific fact sheet setting out the information held by CSNSW is accessible here.

Information may be used in CSNSW for activities such as:

- classification, placement and designation purposes
- visits and telephone call purposes
- processing of applications
- inquiry and complaint handling
- Corrective Services Industries employment purposes
- operation of specialist programs such as drug and alcohol programs, education and vocational training programs
- provision of health services
- assessment (including pre-sentence reports) and case management in correctional facilities and in the community
- administration of custodial and community sentences
- providing access to accredited chaplains and arranging participation in religious observances
- maintaining safe and secure facilities under the control of CSNSW
- law enforcement
- preparation of reports for bodies such as the NSW State Parole Authority (SPA) and the Serious Offenders Review Council (SORC)
- investigations
- processing requests and complaints of individuals and organisations
- restorative justice programs including victim-offender conferencing and mediation, and
- research, evaluation and statistics.

Child Protection and Permanency, District and Youth Justice Services

The Child Protection and Permanency, District and Youth Justice Services division has statutory responsibility for protecting children and young people from harm. Each directorate/district has specific functions.

The directorates/districts include Western Sydney and Nepean Blue Mountains Districts, Hunter and Central Coast Districts, Mid-North Coast, Northern NSW and New England Districts and South Western Sydney District.

The division also oversees Community Services Statewide Services, the Office of the Senior Practitioner, Cross Cluster Operations, Youth Justice and ChildStory.

Child Protection and Permanency

Child Protection and Permanency deals with sensitive information relating to children and young persons and their families. These functions are exercised primarily under the *Children and Young Person's Care and Protection Act 1998* (Care Act).

In terms of information **collection**, this occurs for a range of reasons, such as to support and protect children and families, in response to complaints/enquiries, in addressing allegations of abuse and misconduct, conducting reviews, responding to requests from oversight bodies, for court purposes, and other necessary functions.

What is collected is extensive and varied and can include identifying information, such as:

- name
- date of birth
- information about risk of harm concerns
- health and mental health records
- criminal histories
- records from schools (attendance and progress reports)
- information from funded service providers (counselling reports, assessment records, telephone records, home visit records, meeting records)
- information from online platforms such as Facebook, photographs and video and audio recordings

Personal information is collected verbally (face-to-face or by phone), in writing or through other mediums such as audio/video/photo.

Chapter 16 (and section 248) of the Care Act guides our information collection and exchange when it relates to the safety, welfare or wellbeing of a child or young person and when:

- making decisions, assessments or plans
- initiating or conducting investigations
- providing a service
- managing any risk to the child that might arise in the recipient's capacity as an employer or designated agency

The disclosure of personal information, by Child Protection and Permanency is guided by chapter 16A and 248 (as well as 231V) of the Care Act. Personal information may also be disclosed when the Department is compelled by an oversight agency such as the NSW Ombudsman and Office of the Children's Guardian or for court purposes via a subpoena or warrant.

Youth Justice

Youth Justice uses information collected in order to carry out their functions under relevant legislation, in particular, the *Children (Detention Centres) Act 1987.* Youth Justice may use information for research purposes, the supervision and care of young offenders in Youth Justice centres and in the community including the provision of health, educational and spiritual services, specialised counselling, case management, training in job and living skills. Youth Justice may also use detainee artwork for purposes related to the work of Youth Justice.

Strategy, Policy and Commissioning

NSW Bureau of Crime Statistics and Research (BOCSAR)

BOCSAR's 'unit record data' is used at the lowest level in BOCSAR to evaluate government policies, report performance against government targets such as the Premier's Priority to reduce reoffending and specifically domestic violence reoffending, publish statistical reports etc. For these purposes the unit record data is only ever presented externally in an aggregate de-identified format. The data is also available to external bona fide researchers on request and according to strict conditions. BOCSAR data is never used for operational purposes. It is contrary to the conditions in the Privacy Code of Practice: Bureau of Crime and Statistics and Research for this data to be used for anything other than research.

BOCSAR collects information from Police, Courts, Corrective Services, Youth Justice and Birth, Deaths and Marriages. Personal information is used for demographic breakdowns (age, address etc) as well as linking individuals between data collections (e.g. name, date of birth) when creating the Reoffending Database and now the Linked Data Asset. Additionally, BOCSAR's Criminal Courts collection counting unit reports on 'finalised defendant information' (court information) so personal details such as name are used to link records within the collection.

BOCSAR do not release unit record information with personal details. The exception is research requests with ethics approval for example where a cohort of data including names may be provided to BOCSAR for matching against the Reoffending Database (ROD) and the ROD data is provided back to the researcher along with the names from the original cohort. Another example is the crime victim file which will be provided to the Commonwealth government to build the National Disability Data Asset – this file will include names for adults, but Statistical Linkage Key (SLK) for Youths and is allowed for by the 27B research exemption under the PIPP Act.

BOCSAR use SLK when providing criminal court unit record level data to the Australia Bureau of Statistics

Family and Community Services Insights, Analysis & Research (FACSIAR)

Unit record data is used within FACSIAR to:

- undertake research and analysis
- evaluate government policies and programs
- report performance against government targets such as the Premier's Priorities and State Outcomes
- undertake annual and national reporting.

FACSIAR information is collected as part of our administrative functions in providing services and supports to our clients.

FACSIAR (via I-view, an external data collection agency) undertakes direct data collection as part of the Pathways of Care Longitudinal Study: Outcomes of Children and Young People in Out-of-Home Care (the POCLS). Information is collected about a cohort of children and young people who entered care for the first time between May 2010 and October 2011. Information is collected from children and young people, care givers, teachers and caseworkers. The overall aim of this study is to collect detailed information about the life course development of children who enter OOHC for the first time and the factors that influence their development.

The POCLS has ethics approval from the University of NSW Human Research Ethics Committee (approval number HC10335 & HC16542), Aboriginal Health and Medical Research Council of NSW Ethics Committee (approval number 766/10), NSW Department of Education and Communities State Education Research Approval Process (SERAP, approval number 2012250), and the NSW Population & Health Services Research Ethics Committee (Ref: HREC/14/CIPHS/74 Cancer Institute NSW: 2014/12/570).

Administrative unit record data is available to external researchers on request and under the following strict conditions:

- that the release must be governed by a signed agreement
- a risk assessment is conducted by Information Security to ensure that data/information will be managed appropriately
- there must be a legal basis for releasing the information and there are no identified privacy issues
- approval must be sought from the Data Custodian.

The POCLS de-identified data is stored within the Secure Unified Research Environment (SURE) at the SAX Institute. Access to this information is governed by the ethics approvals and a signed Service Level Agreement.

Housing, Disability and District Services

Housing and Homelessness – Housing State-wide Services (Housing)

Housing uses information about its tenants or applicants for 'directly related' purposes such as:

- the conduct of surveys to monitor client satisfaction
- to train employees
- where it is reasonably necessary for funding, planning or evaluating the provision of a service.

Housing State-wide Services is a central point of contact for:

- The NSW Police Force in relation to information sharing under Section 71 of the *Housing Act 2001* and the *Child Protection (Offender Registration) Act 2000*
- Non-government organisations including Legal Aid and the NSW Trustee and Guardian where client consent has been provided

We share information with the NSW Police Force via the Memorandum of Understanding. Legislation that governs this information sharing includes the *Housing Act 2001*, the *Child and Young Persons (Care and Protection) Act 1998* and *Crimes (Domestic and Personal Violence) Act 2007*.

Along with the NSW Police Force and Corrective Service NSW we share information in order to provide appropriate housing assistance to a registrable person. Legislation that governs this information sharing includes Chapter 16A of the *Children's and Young Persons Care and Protection Act 1998* and Sections 19BA and 21E of the *Child Protection (Offender Registration) Act 2000*. The Guidelines for the Housing of Registrable Persons outlines the arrangements between each organisation in relation to exchanging information on registrable persons seeking housing assistance.

We are also bound to the Commonwealth's Centrelink Confirmation eServices (CCeS) policy in disclosing personal information about our clients or tenants, where the person has consented to that disclosure. The CCeS policy operates within the legislative requirements of the confidentiality provisions contained in various pieces of legislation administered by Centrelink, for example the *Social Security (Administration) Act 1999* and the *A New Family (Family Assistance) (Administration) Act 1999*, as well as the *Privacy Act 1988*.

Boarding House Team

The Department's Boarding Houses Team (BHT) collects Screening Tool of Entry into Assisted Boarding Houses assessments. These are conducted by Australian Unity and provided by email to the BHT in accordance with their funding contract. Screening Tool assessments are a requirement of Clause 14 of the *Boarding Houses Regulation 2013*.

Boarding House Enforcement Officers may need to request information from the NSW Police regarding police attendance at an Assisted Boarding House if they

believe that the manager of the boarding house may be in breach of the Boarding House Regulation and the Act by failing to report the police attendance to FACS. A protocol for this is in place. This information may include:

- date of incident
- full name of resident/s involved in the incident
- reason for the attendance of the police
- outcome of police attendance
- NSW Police Force 'COPS' Event number.

Section 24 of the PPIP Act states that an investigative agency is not required to comply with sections 18 or 19(1) of the PPIP Act if the information concerned is disclosed to another investigative agency. The Department's BHT meets the definition of an 'investigative agency' under the PPIP Act as it is a public sector agency with investigative functions that are exercisable under the authority of an Act, and the exercise of the functions may result in the Department taking or instituting proceedings against a person or body under investigation.

Boarding House Enforcement Officers may also need to make enquiries to establish the needs of a particular person if they are investigating whether any premises is an unauthorised assisted boarding house as defined under section 41 of the *Boarding Houses Act 2012*. In addition, these officers may also need to disclose information about people who are banned from a particular premise to the tenants so that the tenants are able to determine who may enter the premises.

The information collected above is not otherwise disclosed unless there is a legal requirement to do so from another organisation or with legal authority, for example, Ombudsman NSW.

Women NSW

Women NSW (WNSW) aims to improve the lives of all women in NSW by achieving justice and equality through policy, innovation and collaboration. WNSW works with other agencies, community organisations and inter-governmental networks to ensure a fairer, safer and more equitable outcome for all women.

WNSW is involved in several projects, including:

- Men's Behaviour Change Program (MBCP)
- DFV Innovation Fund
- Investing in Women.

In respect of the MBCP, information is collected about the client attending the MBCP, their partner and any dependent children. No names or addresses are collected for any client, partner, ex-partner or children. Dates of birth are collected for

the primary client, that is the male attending the MBCP and ex-partner or current partner. Dependent child/ren DPB information is not collected. The MBCP also operates under a Privacy and Health Code of Practice for the automatic referral pathway which are available at the following links:

- Privacy Code of Practice for the automatic referral pathway
- Health Code of Practice for the automatic referral pathway

The DFV Innovation Fund collects information through a Minimum Dataset Collection tool/spreadsheet. All information is provided voluntarily.

The data for the Investing in Women NSW funding program is collected through a Minimum Dataset Collection tool/spreadsheet. Please note that Service Providers are required to provide input for this program.

Women NSW may use information where reasonably necessary for:

- funding, service design, commissioning, planning
- evaluating the provision of a service, government policies, report performance against government targets such as the Premier's Priority to reduce reoffending and specifically domestic violence reoffending

Inclusion and Early Intervention

The Inclusion and Early Intervention Unit oversees several programs and do not generally collect or store client personal information. This information is handled by program funded service providers, for example the Targeted Earlier Intervention (TEI) Program. Privacy obligations are imposed on funded service providers via their contract with the Department - the Human Services Agreement (HSA) Standard Terms. The HSA stipulates that -funded service providers must comply with privacy legislation PPIP Act, HRIP Act and the Commonwealth *Privacy Act 1988*.

Funded service providers must report data in an IT system called the Data Exchange. This system is hosted by the Australian Government Department of Social Services (DSS). Where an organisation stores personal information in the Data Exchange, only they can access the personal information. Strict IT security protocols prevent DSS employees from accessing personal information for any purpose other than confirming that the privacy protocols are working correctly.

DSS de-identifies and aggregates data in the Data Exchange to produce information for policy development, grants program administration, and research and evaluation purposes. This includes producing reports for sharing with organisations. This information does not include information that identifies clients, or information that can be used to re-identify clients, in any way.

The Department can only access de-identified aggregate data. The Inclusion and Early Intervention Unit uses such information to commission services, understand client needs and to measure the impact of services.

Inclusion and Early Intervention also has responsibilities for **National Disability Insurance Scheme** (NDIS) participants. In relation to handling of personal information for the NDIS:

I. We do not collect any type of information from NDIS participants. The information the Department holds is provided by the National Disability Insurance Agency (NDIA) on fortnightly or monthly basis.

II. We use the NDIS reports to:

   a. monitor and provide summary of NDIS performance to Executives.

   b. perform data analysis to answer queries or provide specific information for specific projects.

   c. data matching with other NSW Agencies (Education, Health, and Transport) for in-kind offsets NSW cash contributions.

III. We only disclose personal NDIS information under known Privacy Codes of Practice and within the NDIA Agreements.

NSW Seniors Card

Seniors Card only collects personal information that is necessary for us to perform our functions and will only use or disclose this information for the purposes for which it was provided. These include providing you with your Seniors Card, annual Discount Directory, mail outs and information about activities for members. Seniors Card may also survey some members in order to improve our services.

The personal information we collect and hold about you includes information you give us when you apply for a Seniors Card or complete an online form on our website. This will include your name, address, date of birth and contact details.

The only personal information which we collect about you when you use our website is what you tell us about yourself, for example, by completing an online form or by sending us an email. We will record your email address if you send us an email.

Seniors Card only use or disclose your personal information for the purpose for which you provided it to us, unless:

- we have your consent to use or disclose your information for that different purpose
- it is required or authorised by law

- permitted by the PPIP Act.

Seniors Card contract out to external service providers some of our functions such as information technology services, mail house services and our call centre. We may provide personal information to these service providers but only so that they can provide the services that we have contracted out to them. External service providers to whom we outsource these functions must sign a confidentiality agreement that prevents them from using your details for any other purpose. If you have consented to receiving special offers you will receive these via the email address you supplied or by post to the mailing address you have supplied as well as ad hoc Public Service Announcements.

NSW Companion Card

Companion Card only collects personal information that is necessary for us to perform our functions and will only use or disclose this information for the purposes for which it was provided. These include providing you with your Companion Card, re-issued Companion Card, direct correspondence relating to your application and updates and newsletters. Companion Card may also survey some members in order to improve our services.

The information collected from applicants or from an authorised third party will be held by the entity that collects it, or by the Department's Business Services. It will be used to deliver services and to meet our legal responsibilities. We may also use your information within the Department as a whole, to plan, coordinate and improve the way we provide services. The Department is also legally authorised to disclose information to outside bodies in certain circumstances. Personal information may also be disclosed to the NSW Registry of Births Deaths and Marriages to ensure cards are valid and issued to recipients with an entitlement. Further information about this can be obtained directly from NSW Companion Card.

Justice Strategy, Policy and Commissioning

Justice Strategy, Policy and Commissioning engage in several programs and services.

The Office for Community Safety and Cohesion is part of this Division and provides services such as:

- the Engagement and Support Program
- the NSW Multi-Agency Case Panel for reintegration of individuals returning from foreign conflict zones
- Security Clearance applications.

In addition to the main classes of information collected by the Department noted earlier in the Plan, the Office of Community Safety and Cohesion also collects information, with the consent of the relevant individuals, from:

- NSW (non-law enforcement) government employees as part of the security clearance vetting process.
- Participants in the NSW Engagement and Support Program which supports vulnerable individuals or at risk of displaying violent extremism behaviours.

Further, information is collected, with appropriate security clearance classification, classified information on individual's returning from foreign conflict zones.

As detailed earlier in this plan, there are applicable exemptions to the PPIP Act relevant to the Office for Community Safety and Cohesion carrying out law enforcement and crime prevention functions.

Law Reform and Legal Services (LRLS)

LRLS includes several business units with varied requirements as to the Information Protection Principles under the PPIP Act.

Office of the Deputy Secretary (including Cabinet Coordination)

The Office of the Deputy Secretary (including Cabinet Coordination) does not collect personal information. However, personal information may from time to time pass through this office in the form of briefing notes, Cabinet and Executive Council minutes. In these cases, the use of this information is consistent with the purpose for which it was collected.

NSW Law Reform Commission and Sentencing Council

The NSW Law Reform Commission & Sentencing Council generally publishes submissions on its website and refers to submissions in its publications. Sometimes submissions include personal information. The NSW Law Reform Commission & Sentencing Council will always seek the consent of the person to whom the information relates before publishing it. When the NSW Law Reform Commission & Sentencing Council accesses personal information as part of a research project, for example, information contained in a confidential court case, the information is always de-identified prior to it being published.

It is the practice of the NSW Law Reform Commission to keep submissions published on their website indefinitely as part of a record of the review process and to assist in the analysis of their reports.

Public Defenders' Office

The Public Defender's Office uses information provided by their clients either via their solicitors or obtained from other sources for the purpose of providing legal representation in serious criminal cases and may collect information in the course of legal representation in courts. The office will only disclose information to other parties representing their clients including the solicitor, any paralegals or when seeking reports from forensic witnesses such as psychiatrists, psychologists or similar. Individuals who are not employees such as students undertaking internships or other placements are required to sign a confidentiality form and are given specific directions on the handling of information.

Legal Services Council

The Legal Services Council has developed their own Privacy Management Plan, which was endorsed by the NSW Privacy Commissioner in December 2019.

Anti-Discrimination NSW

Anti-Discrimination NSW handles personal information in order to administer the *Anti-Discrimination Act 1977 (NSW)* (ADA) which makes it unlawful to discriminate in specified areas of public life against a person on grounds which include their sex, race, age, disability, homosexuality, marital or domestic status, transgender status and carer's responsibilities or vilify on the grounds of race, homosexuality, transgender status or HIV/AIDS status is also unlawful. Personal information is handled in accordance with this Privacy Management Plan and relevant legislative requirements.

Anti-Discrimination NSW is not required to comply with the use and disclosure HPPs in relation to its complaint handling, investigative, review and reporting functions (Schedule 1, clauses 10(3) and 11(3) of HRIPA).

Office of the Legal Services Commissioner

The Office of the Legal Services Commissioner receives and deals with complaints about lawyers or law practices in accordance with the exercise of the Office of the Legal Services Commissioner's statutory functions under the *Legal Profession Uniform Law* (NSW). The Office of the Legal Services Commissioner is subject to a general statutory prohibition on the disclosure of any information obtained in the administration of the *Legal Profession Uniform Law* (see section 462), unless a specified exception applies under section 462(2).

The Office of the Legal Services Commissioner is considered an '*investigative agency*' for the purposes of section 3 of the PPIP Act and is therefore not required to comply with certain provisions of the PPIP Act in accordance with section 24 of the PPIP Act.

Office of the Solicitor General and Crown Advocate

The material in briefs is used for the preparation of submissions to courts and the provision of advice. The material in surveillance device applications is used to consider whether the Attorney General wishes to be heard on a surveillance device application. The material in the requests for the exercise of delegated functions is used in the exercise of those functions.