Privacy Management Plan

Table of contents

1. Introduction

1.1 Purpose

This Privacy Management Plan explains how the Crown Solicitor's Office (CSO) 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 available from on the Information and Privacy Commission website.

This plan sets out the CSO's commitment to respecting the privacy of those whose personal and health 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 CSO 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 how 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 first part of this plan covers how the CSO generally collects and handles personal information.

The *PPIP Act* and the *HRIP Act* contain criminal offence provisions applicable to our employees if they use or disclose personal information or health information without authorisation. We use a range of electronic databases to hold the information we collect, and if an employee 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.

Employee access to CSO databases, including the records management system and practice management system, is strictly for authorised work purposes only.

1.2 What this plan covers

Section 33(2) of the *PPIP Act* sets out the requirements for 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.

1.3 When we review this plan

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

1.4 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 our clients and those whose personal or health information we hold with information about how we meet our privacy obligations.

Additional support for CSO staff in relation to our privacy obligations is available from CSO People & Culture.

1.5 Implementation and training

As part of the onboarding process, all CSO staff complete a mandatory departmental privacy eLearning course. Training is also provided to new CSO staff during their induction, including on the requirements of legal professional privilege and the concomitant obligation not to disclose information obtained in the course of providing legal services.

CSO staff are also responsible for:

- familiarising themselves with and complying with the Privacy Management Plan when dealing with personal and health information
- identifying whether new activities are likely to raise privacy issues and consulting with CSO People & Culture and/or CSO Information Management & Technology, as appropriate
- identifying and raising privacy concerns with their supervisor or Director, or CSO People & Culture and/or CSO Information Management & Technology, as appropriate
- participating in any additional privacy training to improve their knowledge and awareness of privacy obligations.

1.6 Promoting privacy awareness

The CSO takes privacy obligations very seriously and undertakes a range of initiatives to promote awareness 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 Code of Conduct and Fraud and Corruption Control Policy.
- publishing and promoting privacy policies on our intranet
- investigating allegations of breaches of privacy and implementing recommendations made from finalised investigations
- assessing privacy impacts of new activities or processes from the outset.
- modelling a culture of good privacy practice
- educating clients about their privacy rights and obligations in handling sensitive information
- conducting regular privacy training for clients and staff
- publishing regular bulletins that include commentary on recent privacy cases.

Who we are

The CSO is a public service executive agency under the *Government Sector Employment Act 2013* related to the Department of Communities and Justice. The Crown Solicitor is the head of the agency and the solicitor on the record for legal proceedings when representing the State and its agencies. The Crown Solicitor is the sole provider of legal services to the NSW Government in all matters that are regarded as core legal work under Premier's Memorandum 2016-04. The CSO competes with the private sector to deliver non-core legal work to government agencies. The Crown Solicitor does not provide legal services to the public.

More information about the CSO is available on the CSO website.

2. Application of this plan

2.1 Overview of privacy legislation

The *PPIP Act* is concerned with “personal information” and the *HRIP Act* with “heath 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". “Health information” is defined broadly as personal information relating to the health of an individual.

While the definition of “personal information” is broad, there are some important exceptions to the definition. The exceptions most relevant to the CSO is information that:

- is subject of legal professional privilege (see ss 118 and 119 of the *Evidence Act 1995*).
- arises out of a Royal Commission or Special Commission of Inquiry
- is contained in Cabinet documents
- is about an individual's suitability for appointment or employment as a public sector official
- arises 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* and the *HRIP Act* do not mean that other policy or statutory requirements, such as the confidentiality of Cabinet documents, can be disregarded.

The information protection principles and health privacy 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.

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

- Health Privacy Principles (HPPs)
- Information Protection Principles (IPPs).

2.2 Categories of personal and health information collected by CSO

2.2.1 *A. Employees*

CSO collects, retains, and securely stores, personal and/or health information for recruitment, employment, and work, health and safety purposes, including information about:

Type of Information	How/When Collected
Absences from work	Collected through leave applications: ■ Before leave in most instances. ■ After leave for unanticipated leave (such as sick leave).
Conflicts of interest	Collected through questionnaire during onboarding process, and during yearly update survey.
Date of birth	Collected during the onboarding process for records summarising the employment or service history of employees. This includes information maintained in electronic recordkeeping systems.
Education, employment history and qualifications	Collected during onboarding process.
Family and care arrangements	Collected during onboarding process, or in relation to ad hoc Family and Community Services Leave requests.
Financial information for payroll purposes	Ongoing completion in payroll system.
IT Asset allocations / use	Identification of IT assets (laptops /mobile phones) allocated and logging of use of IT systems based on CSO IT acceptable use policy and other IT policies.
Medical conditions, illnesses, and injuries	Collected in relation to sick leave requests and first aid incidents and/or voluntarily disclosed during onboarding process.
Next of kin and contact details	Collected during onboarding process.
Office attendances	Collected through the security access control system
Performance and development	Generated during yearly performance planning and development process.
Secondary employment	Collected through questionnaire during onboarding process, and during yearly update survey.
Workers compensation records	Collected if a workers compensation claim is lodged.

2.2.2 *B. Legal files*

Most of the information held by CSO is contained in our legal files. This information includes clients' instructions, legal advice, and material provided for use in legal proceedings, and is generally subject to legal professional privilege. This information, usually provided by client agencies or legal representatives, may include private or health data related to the parties on the matter.

This information can include:

- birth, death and marriage information
- criminal and incarceration records
- cultural practices
- employment history
- family histories
- financial details
- medical records and reports.

2.2.3 *C. Visitors*

For work, health and safety purposes, a record is kept of individuals who enter CSO offices beyond the public area. This record is kept as a register maintained by CSO Security.

2.2.4 *D. Communications and client engagement*

The CSO maintains mailing lists of client contacts who have asked to be included on these lists. No personal information is collected without consent and those who provide their information are advised as to how CSO will manage it. The information collected generally includes names and contact details.

When the CSO delivers training sessions, it collects details of participants through the registration process. The details collected are generally names and contact details.

2.2.5 *E. Correspondence*

The CSO may hold personal and health information in records of correspondence or other documents sent to the CSO.

Physical documents are digitised by the CSO Service Centre, and the hard copy securely retained until destruction. Digital copies are registered into the CSO records management system with appropriate access controls applied at a matter level.

The Service Centre deals with courier request forms and maintains a register of outgoing Express Post and incoming registered post, which includes the names and contact details of senders and recipients.

2.3 Contracted service providers

The CSO is 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 third parties from unauthorised use or disclosure of personal information that we hold.

Contracts to which the CSO is a party include provisions requiring contractors to deal with personal and health information consistently with the *PPIP Act* and the *HRIP Act*.

2.4 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, personal and health information is collected 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, must be relevant to the function of the CSO, and must not unreasonably intrude into the privacy of an individual.

We maintain business records that contain personal information, including contact details for public officials in other government entities and in third-party organisations. Health information may also be collected and retained. consistent with our obligations under the *HRIP Act*. 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.

2.4.1 *Notification*

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* set 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.

Section 23(2) of the *PPIP Act* specifies exemptions for the requirement to collect directly from the individual concerned when agencies are collecting information in connection with proceedings before any court or tribunal, whether or not proceedings have commenced.

Where information is collected from third parties, the individual is notified in advance, in writing, either as part of the CSO's onboarding process, or by email.

2.5 Employee records

It is a requirement of State Records NSW for the CSO to collect and retain employee records. The *General retention and disposal authority: administrative records (GA28)* identifies common or general administrative records created and

maintained by NSW public offices that are required as State archives, and provides approval for the destruction of certain other administrative records after minimum retention periods have been met.

Employee records (for example leave, attendance, recruitment, and workers compensation) will be held confidentially by CSO People & Culture or the CSO's Shared Services provider until such time as defined by GA28 or any superseding authority issued by State Records NSW.

2.6 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 that personal and health information is stored securely, kept no 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 in our secure computerised databases. The CSO follows strict rules for storing all formats of personal and health information to this information from unauthorised access, loss or misuse.

Personal information and health information, both paper-based and electronic, 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 *State Records Act 1998* (NSW) and the relevant disposal authorities. This link provides a list of relevant Functional Disposal Authorities.

The information we hold, and the communication of this information internally and externally, are subject to the CSO's Information Security Policy and the Classification and Handling of Sensitive Information Policy.

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 IPPs and HPPs.

We require data breaches to be promptly notified to the Director, Information Management & Technology 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.

The CSO's physical files are located on secure floors requiring swipe-card access. Documents that relate to particularly sensitive matters are located separately and require an additional key for access.

The CSO's electronic files require secure login by staff. Files relating to particularly sensitive matters, or containing personal or health information of employees, have access restricted to those staff members required to work on the files.

Where information is stored in a computerised database, CSO naming conventions ensure that appropriate descriptions are used to avoid errors or misinterpretation of data.

Standards have been adopted, with reference to the functions and purposes of the CSO, to ensure personal information is used only for the purposes for which it was collected.

2.7 Access and amendment (*PPIP Act* section 14 -15, *HRIP Act* HPP 7-8)

2.7.1 *Access to personal information*

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.

2.7.2 *Informal requests*

A person wanting to access or amend their own personal or health information can make a request by contacting CSO People & Culture. Generally, this request does not need to be made in writing; however, the request may be reduced to writing 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.

2.7.3 *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 in writing.

CSO People & Culture will aim to respond to the formal application within 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 personnel file. To access their file, employees can email CSO People & Culture.

2.7.4 *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 or health information of another person, an access application should be made under the *Government Information (Public Access) Act 2009* (*GIPA Act*). Further information is available from the Department of Communities and Justice 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.

2.7.5 *Amendment 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 in writing to CSO People & Culture, 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 CSO 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.

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

The *PPIP Act* and the *HRIP Act* place an obligation on the CSO to take reasonable steps, depending on the circumstances to ensure that, having regard to the purpose for which personal or health information held by the CSO 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. 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.

2.9 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. 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 the CSO: for example, if we were to provide information to the NSW Police Force.

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

- the proposed use is consistent with the purpose for which it was collected
- the proposed secondary use is directly related to the purpose of collection
- the individual has consented for use of their personal information for that purpose
- 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 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.]

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

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

- 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.
- 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.
- 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.
- The person concerned has consented to the proposed disclosure.
- It is required for law enforcement or investigation purposes. In such instances, a valid warrant or court order (subpoena) may be required.
- The disclosure is required, permitted, implied, or reasonably contemplated by an act or any other law.
- The disclosure is permitted by a Public Interest Direction or Code made by the NSW Privacy Commissioner.

When information is disclosed by the CSO, it is generally in accordance with a legal obligation (for example, discovery or subpoena) or with consent (such as where a client officer swears an affidavit or statement in the course of legal proceedings).

The CSO does not disclose information for research purposes, except where required to do so. For example, the CSO provides the Office of the Public Service Commissioner with workforce profile data in accordance with the *Government Sector Employment Act 2013*.

2.11 Restricted personal information

The following categories of personal information about an individual are given more stringent protection under section 19(1) of the *PPIP Act*: their ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership and 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*).

2.11.1 *Additional HPPs – identifiers and anonymity*

The *HRIP Act* has an additional HPP (HPP 12) concerning the use of identifiers assigned by organisations to protect individuals' identities. Identifiers are used to uniquely identify an individual and their health records. Agencies can only identify individuals by using unique identifiers if it is reasonably necessary for them to carry out their functions.

HPP 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.

Agencies cannot transfer health information outside NSW or to the Commonwealth unless they reasonably believe the receiving jurisdiction has a similar standard of privacy protection for health information. They must not include health information about any individual in a health records linkage system unless the individual has expressly consented to this.

The CSO does not maintain health records in a linkage system. CSO staff are assigned an employee number, along with their NSW Government Employee Number. CSO staff are not assigned further identifiers.

2.12 Data breaches

Part 6A of the *PPIP Act* establishes the NSW Mandatory Notification of Data Breach (MNDB) Scheme. The MNDB Scheme requires every NSW public sector agency bound by the *PPIP Act* to notify the Privacy Commissioner and affected individuals of eligible data breaches. An eligible data breach 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.

Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches. The CSO's DBP policy outlines our approach to complying with the MNDB Scheme, the roles and responsibilities for reporting data breaches and strategies for containing, assessing and managing eligible data breaches.

The policy applies to all staff and contractors of the CSO. This includes temporary and casual staff, private contractors and consultants engaged by the CSO. The policy also applies to third party providers, who hold personal and health information on behalf of the CSO.

The purpose of the policy is to provide guidance to CSO staff on data breaches of CSO held data in accordance with the requirements of the *PPIP Act*. It sets out how the CSO will respond to data breaches involving personal information. The

CSO acknowledges that not all data breaches will be eligible data breaches but regardless the CSO takes all data breaches seriously. The policy details:

- what constitutes an eligible data breach under the *PPIP Act*
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

In addition, Part IIIC of the *Privacy Act 1988* (Cth) sets out a Notifiable Data Breaches scheme (NDB). The NDB applies to the CSO as a tax file number (TFN) recipient, as we hold TFNs 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.

2.13 Privacy complaints

Any person can make a privacy complaint by applying for an "internal review" of the conduct they believe breaches an IPP and/or an HPP. A person can also discuss concerns with CSO People & Culture.

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.

2.13.1 *Your rights of internal review*

An application for internal review should:

- be in writing
- be addressed to CSO People & Culture
- specify an address in Australia at which you can be notified after the completion of the review.

To apply for an internal review, email CSO People & Culture using a subject line of "Application for Internal Privacy Review", and noting in the body of the email that you wish to apply for an internal review, along with providing your contact address.

2.13.2 *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 qualified to deal with the subject matter of the complaint.

The Director of People & Culture, in consultation with the Director of the Public Law & Commercial (Advisory) practice group, will nominate, for the Crown Solicitor's approval, a suitable person to conduct the review.

The internal review follows the process set out in the Information and 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)
- your 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.

The Privacy Commissioner has an oversight role in the process and may make submissions in relation to the internal review. We will consider any relevant material submitted by the Privacy Commissioner.

Further information about the internal review process is available on the IPC website.

2.13.3 *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 a valid internal review request and 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 NCAT.

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

http://www.ncat.nsw.gov.au/
1300 006 228
Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

2.14 Public Registers

In accordance with the CSO's Gifts, Benefits and Hospitality Policy and the *Government Sector Finance Act 2018*, the CSO makes public a Register of Gifts of Government Property. This Register can be accessed through the CSO's website.

If your personal information is contained in a public register of the CSO, and you wish to apply for suppression of that information, please email the Director, People & Culture.

2.15 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 within the CSO informally before lodging an internal review.

Complaints to the Privacy Commissioner - You 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:

NSW Information and Privacy Commission
Level 15, McKell Building, 2-4 Rawson Place, Haymarket NSW 2000
GPO Box 7011 Sydney NSW 2001
1800 472 679 ipcinfo@ipc.nsw.gov.au

3. Appendix A

Legislation affecting processing of information

Legislation	Details
Crimes Act 1900	Part 6 creates offences for unauthorised obtaining of access to or interference with data in computers. There are higher penalties for accessing certain categories of sensitive government information. For example, law enforcement information or for alteration or destruction of data.
Criminal Records Act 1991	Restricts access to and disclosure of spent and quashed convictions.
Government Information (Public Access) Act 2009	Deals with applications for access to documents which may contain personal information. The *PPIP Act* creates an alternative means of accessing personal information, but the CSO may use limitations and conditions affecting access under the *GIPA Act* when responding to applications for access and correction made under the *PPIP Act*.
Health Records and Information Protection Act 2002	The HPPs establish requirements for protecting individuals' health information (discussed above).
Independent Commission Against Corruption Act 1988	Defines corrupt conduct in a way which has been found to relate to unauthorised disclosure of information for personal benefit.
Privacy and Personal Information Protection Act 1998	In addition to the requirements covered in this Plan, the *PPIP Act* prohibits disclosures of personal information by public sector officers which are not done in accordance with the performance of their official duties. These provisions are primarily directed against corrupt or irregular disclosure of personal information staff may have access to at work and not to inadvertent failure to follow policies and guidelines.
Public Interest Disclosures Act 2022 (*PID Act*)	The definition of personal information under the *PPIP Act* excludes information contained in a protected disclosure. This means that a person cannot seek review of the use or disclosure of a protected disclosure or be prosecuted for unauthorised disclosure of protected disclosure information under the *PPIP Act*. However, the Privacy Management Plan is still able to address strategies for the protection of personal information disclosed under the *PID Act*. Moreover, a "privacy contravention" is a "serious wrongdoing" for the purposes of the *PID Act* (section 13(e))
State Records Act 1998	Defines the circumstances under which the CSO can dispose of its records and authorises the State Records Authority to establish policies, standards and codes to ensure adequate records management by the Department. Compliance with requests to delete irrelevant, inaccurate, or out-of-date information under s. 15 of the *PPIP Act* appears to override the restrictions on destruction under the *State Records Act* (section 20(4)).

4. Appendix B

Policies affecting the processing of information are available to staff through the CSO Staff Manual. Mandated documentation, including this plan, are publicly available online on the CSO's "policies" page.

4.1.1 *Crown Solicitor's Office policies*

- The CSO Code of Conduct reinforces and supplements the requirements of the *PPIP Act* and *HRIP Act*, in particular:
  - Section 5.2.1, dealing with maintaining employee confidentiality and privacy while keeping appropriate records
  - Section 6.10, setting out the confidentiality obligations of staff who have left the Department.
- Data Breach Policy.
- Functional Disposal Authorities.

4.1.2 *External Polices*

The following external documents provide guidance on appropriate ways of collecting, storing, using and disposing of personal information.

NSW Ombudsman's Office

Ombudsman's Effective Complaint Handling Guidelines

Premier's Department

Policy and Guidelines for the Use by Staff of Employer Communication Devices (defines the responsibility of public sector employees in relation to the use of the Internet and electronic mail, available at the Premier's Department).

The Public Service Industrial Relations Guide.

State Records New South Wales

Destruction of Records Guideline

General Disposal Authority Administrative Records (authorises routine disposal of commonly held categories of administrative records in accordance with approved schedules)

Managing Personnel Records (overview with links to disposal schedules)

5. Policy information

Document details

Title:	Privacy Management Plan
Number:	A27
File reference:	AD2014.66.0004
Date of effect:	28 March 2025
Date of last review:	28 March 2025 To be reviewed 11 April 2026.
Security classification:	Official
Policy owner:	Director, People & Culture and Director, Information Management & Technology

Document history

Date	Version	Approved By	Comment
7/7/2015	1	I V Knight, Crown Solicitor	
11/4/2024	2	Karen Smith, Crown Solicitor	
28/3/2025	3	Karen Smith, Crown Solicitor	