Office of the
Children's Guardian

NSW GOVERNMENT

Policy

OCG Privacy Management Plan

May 2024
A8761201

www.ocg.nsw.gov.au

Contents

Privacy Management Plan overview

Purpose

This Privacy Management Plan (**PMP**) tells our stakeholders, members of the public, and our staff about how the Office of the Children's Guardian (**OCG**) handles personal and health information in line with NSW privacy laws. The PMP also acts as a guide to OCG staff on how to comply with these laws. These laws are:

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

The PMP provides contact details to assist members of the public with questions about their personal information, or if they wish to access and/or amend the personal and health information we hold.

We also have a legal obligation to tell members of the public and our stakeholders about their rights under NSW privacy laws to complain about or seek review of our conduct. The PMP does this by providing detailed information about what to do if a person thinks that the OCG may have breached the PPIP Act or HRIP Act.

What this PMP covers

The PMP complies with the legislated requirements for a Privacy Management Plan under section 33 of the PPIP Act. Section 33(2) of the PPIP Act requires the PMP to include:

- information about how the OCG devises policies and practices to ensure compliance with the requirements of the PIPP Act or the HRIP Act
- how we disseminate these policies and practices to staff within the organisation
- our internal review procedures
- any other matters which we consider relevant in relation to privacy and the protection of personal and health information we hold.

The key terms used in this PMP are set out in the table at **'Appendix A'**.

The PMP covers all OCG business units. While each business unit has unique functions and does various types of work, this PMP applies in the same way to all units.

One shared obligation across all business units is in bringing to attention privacy breaches, including, how the OCG deals with data breaches.

Separate from this PMP, the OCG has a Data Breach Policy that sets out the OCG's procedures and practices for managing a data breach, including the assessment and notification requirements for the Mandatory Notification of Data Breach Scheme set out in Part 6A of the PIPP Act. The PMP should be read together with the Data Breach Policy.

Review of PMP

The Director, Corporate Services is responsible for maintaining the PMP by reviewing and updating the plan, and for informing OCG business units and staff of any changes to the PMP.

We will review the PMP every two years. We will also update the PMP from time to time to respond to any amendments to NSW privacy laws or other laws that impact personal information, or any changes in our practices in dealing with personal and health information.

Whenever we review our plan, we will provide a copy to the Privacy Commissioner as soon as practicable after it is amended.

OCG Privacy Officer

The OCG's General Counsel is the delegated OCG Privacy Officer and leads a team in the General Counsel Directorate that is responsible for:

- providing or arranging for privacy training and awareness raising activities to OCG staff
- responding to enquiries from OCG staff and members of the public about how the OCG handles personal and health information
- providing guidance on compliance with Information Protection Principles (**IPPs**) and Health Privacy Principles (**HPPs**), including providing in-house advice on managing privacy risks
- handling general privacy complaints referred by the OCG's Director, Corporate Services
- conducting internal reviews under section 53 of the PPIP Act for complaints about the OCG's conduct under the PPIP Act and HRIP Act
- communicating with the Information and Privacy Commission on any legal matters if required.

For any questions about the PMP, or the OCG's privacy obligations, please contact the OCG Privacy Officer by email at Legal@ocg.nsw.gov.au.

Strategies for implementing this plan

Policy and practices development

The OCG develops policies and other guidance to support our practices in handling personal and health information. The OCG develops policies and practices by:

- identifying whether new projects or systems are likely to raise privacy issues, and taking action to address those issues, such as seeking legal advice from the General Counsel Directorate and implementing a privacy impact assessment of the project or system
- examining changes in the legislative, policy or operational environment and their impacts on our privacy management practices
- reviewing and updating policies and procedures for handling personal and health information
- responding to concerns or views raised by staff, members of the public, or other stakeholders about our practices
- engaging with the Information and Privacy Commission (**IPC**) on our compliance with its information privacy obligations, and adopting regulatory advice published by the IPC
- considering the privacy implications of our work and promoting change to any workplace practices, policies and systems for storing and accessing personal information.

The OCG Privacy Officer will consult business units when reviewing and developing privacy management policies or practices. The OCG Privacy Officer will consult the OCG's Media and Communications unit to communicate across the agency any new policies or key amendments. This ensures staff are made aware of their obligations under the PPIP Act and HRIP Act.

Dissemination of policies and practices

The OCG undertakes a range of initiatives to ensure our staff and members of the public are informed of our privacy practices and our strategies for building agency wide compliance with our obligations under the PPIP Act and HRIP Act.

We broadly promote our privacy policies and procedures across our agency so that all staff are aware of our privacy practices, and apply these to their work.

Our PMP explains legal terms in the PPIP Act and the HRIP Act so that people can use this plan to help them understand our obligations under privacy laws.

We aim to communicate clearly in our policies and procedures and other guidance so that staff can apply those procedures to their work involving personal and health information.

We advise staff of what to do if they are unsure of procedures or have concerns about whether they are complying with the PPIP Act or HRIP Act.

We promote privacy awareness and compliance of privacy practices and obligations amongst staff members by:

- writing the PMP in plain English
- publishing the PMP prominently on the OCG's website for the public, and on the intranet for access by staff
- providing privacy training to improve understanding and awareness of privacy obligations, including, targeted training for staff who work in business units with a higher exposure to personal or health information
- incorporating privacy obligations and compliance into business plans or in the design of projects
- encouraging staff members to consult their supervisors if they identify a potential privacy issue
- encouraging staff members to seek advice from the OCG Privacy Officer or the OCG's General Counsel's Directorate.

We promote public awareness of the PMP by:

- writing the PMP in plain English and avoiding legal jargon
- publishing the PMP prominently on the OCG website so it is easily available to the public
- providing hard copies of the plan free of charge on request
- referring people to the PMP when responding to public enquiries
- referring to the PMP in our privacy collection notices.

We make this plan available to members of the public on our website at: https://ocg.nsw.gov.au/privacy

Stakeholders and members of the public may request a hard copy of this plan by contacting the OCG at (02) 8219 3600.

Governance

Our Executive team promotes a culture of good privacy practice by supporting our agency to comply with the PPIP Act and HRIP Act by:

- endorsing the PMP and making it publicly available
- endorsing privacy training for staff, and incorporating privacy obligations and compliance into business plans

- providing a copy of the plan to our internal oversight bodies such as the Audit and Risk Committee
- making privacy awareness and compliance a standard agenda item in executive meetings
- consulting the OCG Privacy Officer on any matters that impact OCG's compliance with its privacy obligations
- providing a statement in our annual report of the action taken by the OCG to comply with the requirements of the PPIP Act, and statistical details of any review we conduct under Part 5 of the PPIP Act, in line with the *Annual Reports (Departments) Regulation 2015*.

About the OCG

The OCG is an independent statutory authority established under the *Children's Guardian Act 2019* (**CG Act**). The CG Act gives the Children's Guardian their principal functions and the OCG its key responsibilities, including:

- promoting the quality of child safe practices
- regulating organisations and individuals providing services to children in NSW
- educating employers and organisations about their responsibilities
- monitoring organisations and individuals to achieve ongoing, child-centred culture and compliance
- facilitating sector-wide cultural change to work practices to achieve safe places for children.

Our statutory functions mean we have range of obligations and deal with diverse stakeholders. Our stakeholders include:

- members of the public
- individuals who hold or apply to hold a worker check and/or their legal representatives
- NSW public sector agencies
- non-government organisations
- not-for-profit sector.

The OCG operates within a framework of the following legislation relating to child protection:

- Children's Guardian Act 2019
- Children's Guardian Regulation 2022
- Children and Young Persons (Care and Protection) Act 1998
- Children and Young Persons (Care and Protection) Regulation 2022
- Child Protection (Working with Children) Act 2012
- Child Protection (Working with Children) Regulation 2013
- Adoption Act 2000
- Adoption Regulation 2015

The principal functions of the Children's Guardian are set out in section 128 of the CG Act:

- exercising functions relating to persons engaged in child-related work, including Working with Children Check clearances, under the WWC Act
- administering the reportable conduct scheme and working with relevant entities to prevent, identify and respond to reportable conduct and promote compliance with the scheme

- taking action to build the capability of child safe organisations to implement the Child Safe Standards, and to monitor, investigate and enforce the implementation by child safe organisations of those Standards
- exercising functions relating to the employment of children, including the making and revocation of exemptions from the requirement to hold an employer's authority
- ensuring the rights of all children and young persons in out-of-home care are safeguarded and promoted
- establishing and maintaining a register for the purpose of the authorisation of individuals as authorised carers
- establishing and maintaining a register for the application and engagement of individuals as residential care workers
- accrediting designated agencies and adoption providers, and to monitor their functions
- developing and administering a voluntary accreditation scheme for persons working with, and programs for, persons who have committed sexual offences against children.

The OCG also has legal obligations under various laws for how it manages information. These obligations include, how the OCG stores records, shares records with other government sector agencies, and receives and decides applications made for access to information, including, personal and health information. The laws include:

- State Records Act 1998
- Government Information (Public Access) Act 2009
- Government Information (Public Access) Regulation 2009
- Privacy and Personal Information Protection Act 1998
- Health Records and Information Privacy Act 2002
- Data Sharing (Government Sector) Act 2015.

As well as these, the OCG may also be subject to privacy codes of practice or public interest directions which are implemented under the PPIP Act. Currently, we are not subject to any of these.

We also comply with various NSW Government policy concerning digital information and cyber security. This includes:

- NSW Government Digital Information Security Policy
- NSW Cyber security policy.

For more details about the OCG's functions and this legal framework, please visit our website at www.ocg.nsw.gov.au

What is personal and health information?

Personal information is defined in section 4 of the PPIP Act as:

- information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about a person where that person's identity is apparent or can be reasonably ascertained from the information or opinion
- personal information can include such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

A person's name and address are clear examples of personal information.

We may also hold personal information in visual formats, including photographs and digital images.

Health information is generally excluded from the definition of 'personal information' in the PPIP Act, as it is covered by the HRIP Act. As defined in section 6 of the HRIP Act, health information means:

a) personal information that is information or an opinion about:

   i) the physical or mental health or a disability (at any time) of an individual, or

   ii) an individual's express wishes about the future provision of health services, or

   iii) a health service provided, or to be provided, to an individual, or

b) other personal information collected to provide, or in providing, a health service, or

c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or

d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or donation, genetic information, or

e) healthcare identifiers,

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

The types of records which contain health information include, a psychologist's report, blood test results, X-ray, or information in a person's medical file. It can also include some personal information that is collected to provide a health service to the person.

The OCG may not hold all the types of health information that is set out in the definition above. However, the OCG does receive health information about individuals in the exercise of its functions, including, when it is lawfully authorised by the CG Act to obtain information from a person. The OCG may also collect health information about employees in the exercise of work performed by the OCG's People and Culture team.

The PPIP Act and HRIP Act provides exceptions to these definitions of personal information and health information. For example, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official, does not constitute personal or health information for the purposes of the PPIP Act and HRIP Act.

Types of information we hold

Due to the OCG's diverse functions and activities, we hold a broad range of personal and health information. This may be contained within the following types of records:

- personnel and employment records
- records created in the exercise of our functions and work activities, for example, information in reports or investigation findings and notices
- legal files (including legal advice)
- correspondence with stakeholders or other agencies
- information relating to assessments, reviews, and investigations conducted by the OCG or other organisations and agencies
- information relating to notifications and complaints received by the OCG

- information received from other government organisations/agencies, the private sector and the general public (including submissions and consultation responses)
- information recorded on registers maintained by the OCG.

The personal information we hold includes information that helps us to identify a person, for example, an individual's, name, address, date of birth, contact details, and proof of identity information. We also hold information about a person's physical or mental health or disability, financial information, academic and professional qualifications, and opinions.

Information may also reveal a person's circumstances or experiences which are highly sensitive, such as their employment history or complaints or performance. The OCG applies the standards of protection under the IPPs and HPPs to all information and takes seriously its obligations to safeguard the information that it holds.

Further detail is at Appendix B and Appendix C.

Overview of our privacy obligations

OCG obligations under the PPIP Act

As the OCG is a 'public sector agency' under the PPIP Act, we are bound by that Act when we collect, store, use and disclose personal information. The PPIP Act through its IPPs sets out the expectations for how we handle and manage personal information in the exercise of our functions under the child protection laws set out above.

The PPIP Act also recognises that some of our functions, for example, functions under the reportable conduct scheme in Part 4 of the CG Act, make us an 'investigative agency' for the purposes of the PPIP Act. That means we may be exempt from complying with some IPPs if compliance might detrimentally affect (or prevent the proper exercise of) our investigative functions.

The PPIP Act also identifies the functions of the Children's Guardian in other ways which can exempt the OCG from complying with the IPPs for certain information. This may be, for example, where the OCG may be permitted to disclose personal information if this is lawfully required.

Our staff (employees) are considered 'public sector officials' under the PPIP Act. Certain information that we hold about an individual's suitability for appointment or employment as a public sector official, is not considered personal information. We may have to use that information for our recruitment purposes or professional development or even internal management of complaints. We handle all information about our staff professionally, including in how we use or disclose this information.

As 'public sector officials' our staff must also work to the standards of conduct expected by the IPPs and we assist our staff to achieve this. We will ensure staff are made aware of their privacy obligations and by providing training to inform and to grow staff capability.

The PPIP Act makes it an offence for public sector officials to misuse or disclose personal information outside the proper exercise of their employment functions for the OCG. See, Offences under the PPIP Act and HRIP Act.

The PPIP Act also provides for review of conduct under Part 5. Our conduct against the IPPs may be subject to internal review, including by way of our Privacy Officer conducting independent internal review of complaints. These reviews must also be notified to the Privacy Commissioner who can make submissions on the review.

Our conduct may also be subject to external review by the NSW Civil and Administrative Tribunal (**NCAT**) which can make binding orders on the OCG to take action if we have breached the PPIP Act. See Options for Seeking Review.

OCG obligations under the HRIP Act

The OCG must also comply with the HPPs set out by the HRIP Act in protecting the health information that it holds. This includes health information obtained about individuals in the exercise of the OCG's statutory functions, and also includes health information about OCG staff.

The OCG's conduct in dealing with health information may also be reviewed under Part 5 of the PPIP Act, as set out above.

Other privacy obligations

We may also have privacy obligations under public interest directions and a Privacy Code of Practice. These are made under the PPIP Act and can modify how the IPPs and HPPs apply to the OCG's privacy obligations. There are currently no public interest directions or codes of practice that are directed at the OCG's functions or particular projects, or likely to affect how the OCG manages personal and health information.

A summary of other laws that direct how the OCG deals with personal and health information or, identify offences involving the misuse of personal information is at Appendix D.

For more information about privacy laws, please refer to our website at https://ocg.nsw.gov.au/privacy

Summary of our privacy obligations

Our privacy obligations are condensed into the following principles.

Table 1. Privacy obligations

Collection	Exemptions
We collect personal and health information lawfully, and only where reasonably necessary for purposes directly related to our functions and activities (**s.8 PPIP Act / Sch 1 cl.1 HRIP Act**).	None
We collect personal information from the individual to whom the information relates unless the individual has authorised collection of the information from someone else (**s.9 PPIP Act**).	We are not required to comply with this principle if: - regarding personal information, the information is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal (**s.23(2) PPIP Act**). - regarding personal information, compliance might detrimentally affect (or prevent the proper exercise of) our complaint handling functions or any of our investigative functions (**s.24(1) PPIP Act**). - regarding personal information, we

	are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**s.25 PPIP Act**).
We collect health information from the individual to whom the information relates unless it is unreasonable or impracticable to do so (**Sch 1 cl. 3 HRIP Act**).	None
We take reasonable steps to inform individuals why their personal and health information is being collected, what the information will be used for, and to whom it will be disclosed. We tell individuals how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to us (**s.10 PPIP Act; Sch 1 cl. 4 HRIP Act**).	We are not required to comply with this principle if: - regarding personal information, the information concerned is collected for law enforcement purposes (**s.23(3) PPIP Act**). - regarding personal information, compliance might detrimentally affect (or prevent the proper exercise of) our complaint handling functions or any of our investigative functions (**s.24(1) PPIP Act**). - we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**s.25 PPIP Act / Sch 1, cl. 4(4) HRIP Act**).
We take reasonable steps to ensure that the personal and health information we collect is relevant, is not excessive, accurate, up to date and complete. We also ensure the collection of information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates (**s.11 PPIP Act / Sch 1 cl. 2 HRIP Act**).	
Storage	**Exemptions**
We store personal and health information securely, keep it for no longer than is necessary for which the information may lawfully be used, and destroy it appropriately. We ensure information is protected by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, unauthorised use and unauthorised disclosure (**s.12 PPIP Act / Sch 1 cl. 5 HRIP Act**).	Regarding health information, we are not required to comply with this principle if we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**Sch 1, cl. 5(2) HRIP Act**).
Access	**Exemptions**

We are transparent about the personal and health information we hold, why we use the information, and the person's entitlement to gain access to the information (**s.13 PPIP Act / Sch 1 cl. 6 HRIP Act**).	We are not required to comply with this principle if: - regarding personal information, compliance might detrimentally affect (or prevent the proper exercise of) our complaint handling functions or any of our investigative functions (**s.24(1) PPIP Act**). - we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**s.25 PPIP Act / Sch 1 cl. 6(2) HRIP Act**).
Upon the request of the individual to whom the personal and health information relates, we provide the individual with access to the information without unreasonable delay or expense (**s.14 PPIP Act / Sch 1 cl. 7 HRIP Act**). -	We are not required to comply with this principle if: - regarding personal information, compliance might detrimentally affect (or prevent the proper exercise of) our complaint handling functions or any of our investigative functions (**s.24(1) PPIP Act**). - we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**s.25 PPIP Act / Sch 1 cl. 7(2) HRIP Act**).
Upon the request of the individual to whom the personal and health information relates, we allow the individual to update, correct, or amend their personal and health information where necessary (**s.15 PPIP Act / Sch 1 cl. 8 HRIP Act**).	We are not required to comply with this principle if: - regarding personal information, compliance might detrimentally affect (or prevent the proper exercise of) our complaint handling functions or any of our investigative functions (**s.24(1) PPIP Act**). - we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**s.25 PPIP Act / Sch 1 cl. 7(2) HRIP Act**).
Use	**Exemptions**
We ensure that the personal information we use/propose to use is relevant, accurate, up to date, complete and not misleading (**s.16 PPIP Act / Sch 1 cl. 9 HRIP Act**).	None
We only use personal and health information for	We are not required to comply with this

the purpose it was collected unless:

- the individual to whom the information relates consents to the information being used for a purpose (**secondary purpose**) other than the purpose for which it was collected (**primary purpose**), or
- the secondary purpose is directly related to the primary purpose and the individual would reasonably expect us to use the information for the secondary purpose, or
- we believe on reasonable grounds that use of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person, or
- the use of information for the secondary purpose is reasonably necessary for the exercise of our complaint handling and investigative functions (**s.17 PPIP Act / Sch 1 cl. 10 HRIP Act**).

principle if:

- regarding personal information, the use of the information concerned for a purpose other than purpose for which it was collected is reasonably necessary law enforcement purposes or for the protection of the public revenue (**s.23(4) PPIP Act**).
- regarding personal information, use of the information for a purpose other than the purpose for which it was collected is reasonably necessary in order to enable us to exercise our complaint handling functions or any of our investigative functions (**s.24(2) PPIP Act**).
- we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**s.25 PPIP Act / Sch 1 cl. 10(2) HRIP Act**).

Disclosure	Exemptions
We will not disclose personal information to a person (other than the individual to whom the information relates) or other body, unless: - 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 - the individual concerned is reasonably likely to have been aware, or has been made aware when the information was collected, that information of that kind is usually disclose to that other person or body, or - we believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person (**s.18 PPIP Act**).	Regarding personal information, we are not required to comply with this principle if: - the disclosure of information concerned is made in connection with proceedings for an offence or for law enforcement purposes, or is required by subpoena or other statutory instrument, or is reasonably necessary for the protection of the public revenue, or in order to investigate an offence where there are reasonable grounds to believe than an offence may have been committed (**s.23(5) PPIP Act**). - compliance might detrimentally affect (or prevent the proper exercise of) our complaint handling functions or any of our investigative functions (**s.24(1) PPIP Act**). - the information is disclosed to another investigative agency (**s.24(3) PPIP Act**). - non-compliance is reasonably necessary to assist another public sector agency that is an investigative agency in exercising its investigative functions (**s.24(4) PPIP Act**).

	- the information is disclosed to a complainant and the disclosure is reasonably necessary for the purpose of reporting the progress of an investigation into the complaint made by the complainant, or providing the complainant with advice as to the outcome of the complaint or any action taken as a result of the complaint (**s.24(5) PPIP Act**). - we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law (**s.25 PPIP Act**).
We will not disclose health information for a purpose (**secondary purpose**) other than the purpose it was collected (**primary purpose**), unless: - the individual to whom the information relates has consented to the disclosure of the information for the secondary purpose, or - the secondary purpose is directly related to the primary purpose and the individual would reasonably expect us to disclose the information for the secondary purpose, or - we believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of the individual concerned or another person, a serious threat to public health or public safety, or - the disclosure of information for the secondary purpose is reasonably necessary for the exercise of our complaint handling and investigative functions (**Sch 1 cl. 11 HRIP Act**).	Regarding health information, we are not required to comply with this principle if we are lawfully authorised or required not to comply with the principle, or non-compliance is otherwise permitted under an Act or any other law, or we (as an investigative agency) disclose information to another investigative agency (**Sch 1 cl. 11(2) HRIP Act**).
We do not disclose, without consent, sensitive personal information such as ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership (**s.19 PPIP Act**).	Regarding personal information, the PPIP Act provides that we are not required to comply with this principle (**s.28(1) PPIP Act**).

How we manage personal and health information

This section of the PMP provides a general overview of how the OCG manages personal and health information when carrying out its functions and activities. A description of our statutory functions and activities is set out at Appendix B and Appendix C.

In this section, we explain how we comply with the IPPs and the HPPs in our information handling practices.

We use the term 'manage' to mean how the OCG collects, stores (and disposes), uses, discloses, provides access to personal information. Sometimes we refer to this as our 'conduct'.

A reference to 'personal information' includes a reference to 'health information'.

You can obtain a more detailed explanation of the IPPs and the HPPs by referring to the table in Our privacy obligations (above) which sets out the circumstances where the OCG is exempt from complying with the privacy principles.

Collection

'Collection' means the way in which the OCG obtains personal or health information.

We collect information in different ways, including in writing, in an email, a verbal conversation, a voice recording, photos or scanned images, or through on-line forms on the OCG's website.

We collect personal information from all our stakeholders, such as members of the public, other NSW public sector organisations/agencies, the private sector, and non-government organisations.

Generally, the IPPs require us to collect personal information directly from the individual. However, we are sometimes permitted to collect information from another person, such as a legal representative or a support person, if that person is authorised to provide the information to us.

As a matter of practice, we ask the individual to first provide a signed authority which permits the OCG to correspond with the representative or support person to collect information. This is also important before we provide information to an individual's legal representative or support person about the individual's matter.

In some circumstances, we may rely on an exemption to the privacy collection principle under the PPIP Act. For example, under section 25 of the PPIP Act, we are not required to comply with certain IPPs if we are lawfully authorised or required not to comply with the principle concerned.

We must ensure that an accurate record of the personal information is collected from individuals. If we collect information verbally, we are required to put any information collected into written form. For example, if an OCG officer collects the information from the individual during a telephone conversation, the OCG officer will record the information in a written file note during the conversation, or close in time afterwards if it is not practical to do this at the time of collection.

We only collect personal and health information by lawful means, and only if it is reasonably necessary for purposes directly related to our functions and activities. We take active measures to ensure that the collection of personal information is relevant, not excessive, and is not an unreasonable intrusion into the affairs on an individual.

Privacy collection notices and consent

We ensure business units use privacy collection notices that advise the purposes for which the information is being collected and that this collection is relevant to their business functions. When we issue requests to external organisations or individuals to obtain information about an individual, we ensure that the scope of the request is limited to information relevant to the work conducted by the business unit.

The collection principle also requires us to tell a person certain information about why we are collecting their personal information. We give a privacy notice to the individual to tell them about the purpose for collection, who we intend will receive the information, whether the information is required by law, and if there is any consequence for not providing the required information. We must not use personal information for a purpose other than that for which it was collected unless the individual to who the information relates has consented to the use of the information for that other purpose, or an exception or exemption to the principle applies.

Storage

The OCG stores personal information in its various record keeping systems, including:

- electronically on databases, such as data entries and file noting
- in documents attached to electronic files stored in electronic record systems
- hard copy documents and files located at our office or stored by third party providers that hold information on behalf of the OCG (for example, the Government Records Repository).

Safeguarding access to OCG offices

We also control how access to records is given and we limit access to our staff. We do this by having in place access restrictions at our office locations. Our staff can only access our office by key card access to our office. Visitors cannot enter without our permission, and we do not leave visitors unsupervised when they are in our office. Our office is locked outside of business hours.

The OCG practices a 'clean desk' approach at its office locations, which means that hard copy files are placed in secure locked cabinets at the end of the working day or when not they are no longer being used. We use secure printing at our office to avoid personal or sensitive information being left on display at printers.

We do permit OCG staff to access our records from locations outside the office (for example, working from home arrangements). We also permit our staff to take electronic or hard copy files off-site to perform their work (for example, attending proceedings at court or tribunals, or attending the premises of another organisation). Our staff are advised not to leave sensitive files unattended and not to let anyone else have access to them.

We have retention and disposal rules for our records in line with the *State Records Act 1998*. We archive older physical files in a secure storage facility in compliance with that Act. When personal information in paper-based documents is no longer needed, OCG staff dispose of the documents in locked bins that are specifically designated for secure destruction.

Electronic records and databases

All our electronic information is stored on secure information systems from our corporate service provider. The systems comply with the international standard of information security ISO/IEC 27001 as per our Information Security Management System (ISMS) Policy. Our servers are backed up daily. Only authorised staff are given permission to access the databases and information management systems through password-protected login.

Our electronic databases and general information management systems include:

- the Working with Children Check (WWCC) Register, which is a database containing information about WWCC applicants and holders
- the Carer's Register, which is a centralised database containing information about people who are, or who have applied to become an authorised carer
- the Residential Care Workers Register, which is a centralised database containing information about people who are, or who have applied to become, residential care workers
- PEGA system
- Objective document management system
- Resolve document management system.

We have safeguards in place for promoting the security of our record systems. This includes controlling how staff access our networks so as to avoid inappropriate or unnecessary access. These include:

- requiring OCG staff to log in by way of multi-factor authentication

- requiring OCG staff to have unique user accounts and passwords to access our computer systems
- automated password updates so OCG staff regularly change their computer login password
- advising staff to not give their passwords to anyone or let anyone else use their computer login.

Our databases or information management systems may also secure information by restricting access to certain files or documents. Access to this information is only granted by approval from the staff member's manager or the Director of the relevant business unit.

Business units consult the OCG's General Counsel Directorate about new information management systems and software. We do this to make sure that any new system will comply with the security and retention principles for personal information under the PPIP Act. We must provide safeguards that are reasonable to protect personal information and we give priority to addressing any concerns about the security of our existing or new record systems.

Security and storage by OCG contracted service providers

Where it is necessary for personal or health information to be transferred to a third party 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 PPIP Act and the HPP Act, and information security policies.

Access and Accuracy

We aim to be transparent with our stakeholders by telling the public about the type of information we hold. We also tell the public how to access this information. We mainly do this through the OCG's website and the OCG's Agency Information Guide, which can also be found on the OCG's website here: https://ocg.nsw.gov.au/about-us/access-information

We aim to ensure that personal information is accurate, up to date, and complete before using it. For example, when we discuss a working with children clearance application, we ask the person to verify their personal information (for example, address or email address) and provide us with any changes to their information. OCG staff within the relevant business unit are authorised to make appropriate amendments to general personal information (such as contact details) when a request is made by the person.

Please see How to access your personal and health information and 'Amendment of personal or health information' (below) for further information about how the OCG provides people with access to the personal information we hold about them, and how they can make a request to amend their personal information.

Use

The OCG uses the information it collects for the purpose of exercising the functions of the Children's Guardian and in performing the OCG's activities. As a general principle, we use the personal information we have collected only for the purpose for which it was collected.

Before we use the personal information, we consider:

- whether the person to whom the information relates has consented to the proposed use
- whether the proposed use is for the purpose for which the information was collected
- if we use the information for a secondary purpose, whether that is directly related to the purpose of collection
- we check the accuracy of the information that we propose to use.

The table in Our privacy obligations (above) sets out the circumstances where the OCG is exempt from complying with the privacy principles concerning use of personal information. If OCG staff propose to rely on an exemption, or if they are in doubt as to whether personal information can be used for any other purpose, they are encouraged to consult the OCG's General Counsel Directorate prior to using the information.

Disclosure

Put simply, the OCG discloses personal information when it gives the information to someone who did not previously have the information.

The OCG mainly discloses personal information to individuals or bodies outside the OCG that are directly related to the functions for which the information was collected. For example, the proposed disclosure is explained in a privacy collection notice, such as the need to disclose the information to a third party so that the OCG is able to perform its functions or activities.

Some disclosures of information may be permitted even where the disclosure is for another purpose or without the person's consent. If OCG staff propose to rely on an exemption to the disclosure principles, or if they are in doubt as to whether personal information can be disclosed for any other purpose, they are encouraged to contact the OCG's General Counsel Directorate and seek advice. This should happen before deciding to disclose the information.

We have in place safeguards to avoid disclosing information in error, such as by checking whether the address in correspondence matches the correct recipient before it is sent.

We continue to develop our procedures and work practices to protect personal information from such disclosures. We refer to guidance published by the Privacy Commissioner through the office of the IPC.

Notification of data breaches

A data breach may occur where there is a failure to protect personal information held by the OCG from being lost or being subject to unauthorised access or disclosure. This may be by human error, including by OCG staff, or by malicious intent by a third party, for example a cyber attack. Examples may include:

- accidental loss of a paper record, or a laptop or USB stick which provides access to electronically stored records
- sending emails to the wrong recipients, including emails which contain attached documents
- cyber attacks such as malware, hacking and data theft.

We respond promptly to data breaches, as it can reduce the impact of a breach on individuals and the OCG, and may prevent future breaches. The OCG's processes and procedures for managing data breaches, including practices to ensure compliance with the obligations and responsibilities under Part 6A of the PPIP Act (Mandatory Notification of Data Breach Scheme), are set out in our Data Breach Policy.

Offences under the PPIP Act and HRIP Act

Our NSW privacy laws recognise that unfortunately sometimes corrupt conduct may occur by the misuse of a public official's functions. A public sector employee, may, for example, misuse their official position to unlawfully access personal or health information. Both the PPIP Act and the HRIP Act make clear that a public official must not allow themselves to be induced by another person to supply personal or health information.

Under section 62 of the PPIP Act:

- it is an offence for a public official (for example member of staff) to intentionally disclose or use personal information accessed in their official functions in doing their job
- a person must not induce or attempt to induce a public sector official (by way of a bribe or other similar corrupt conduct) to disclose any personal information about another person to which the official has or had access in the exercise of their official functions.

Section 58 of the HRIP Act provides the same offences for health information.

Under section 63 of the PPIP Act it is also an offence for a person to supply personal information that the person knows, or ought reasonably to know, has been or is proposed to be disclosed in contravention of section 62. Section 69 of the HRIP Act provides the same offence for health information.

Other offences include:

- under section 68 of the PPIP Act, there are a range of offences relating to how a person deals with the NSW Privacy Commissioner, including such things as to hinder the Privacy Commissioner or a member of staff from doing their job
- under s. 70 of the HRIP Act, there are certain offences relating to threatening or intimidating behaviour to, for example, prevent a person from requesting access to health information, or require another person to give consent, or to do, without consent, an act for which consent is required.

OCG safeguards

We have obligations to provide reasonable safeguards to prevent this type of conduct. For example:

- taking steps to ensure that staff are aware of our policies on the requirements of the IPPs and the HPPs and we require staff to comply with those policies
- restricting access to certain databases as a safeguard to prevent authorised access
- encouraging staff members to seek advice from the OCG's General Counsel Directorate if there is uncertainty about use or disclosure of information.

How to access your personal and health information

Any person has the right to request access to personal information we hold about them. This may be where a person wishes to know what type of information we hold, or if they wish to correct or amend the information.

The right to request access to personal information is given by the PPIP Act under the access IPP in section 14; and the right to request access to health information is given by the access HPP in clause 7 of Schedule 1 to the HRIP Act.

The PPIP Act and the HRIP Act do not set any requirements for how a person is to request access to information. There is no fee for making a request under the PPIP Act. The OCG does not charge any fees for dealing with requests for personal or health information.

While a request does not have to be in writing, we encourage people to write to us about the request so that we can ensure that we have a record of your request and can identify the information.

In responding to a request, both the IPPs and the HPPs require the OCG to provide access to personal or health information without excessive delay or expense.

Where to make a request for personal information

We aim to assist people by making access to information as informal as possible.

A person can contact the relevant business unit or staff member within the OCG. To ensure the request is received by the business unit or OCG staff member, please refer to the table below for guidance.

Table 2. Where to make a request for personal information

Information type	Contact
Case-related	If you are requesting information about a case in which you are personally involved, you can contact the business unit or staff member handling the matter (for example, WWCC Directorate, Reportable Conduct Directorate).
Staff records	If you are an OCG staff member, you can contact the OCG's People and Culture team. **Note:** OCG staff can use the SAP system to amend their own personal details (for example, contact details, bank details), without the need for a request.
Other enquiries	OCG's main enquiry line (Ph: 02 8210 3600) or email ocg@ocg.nsw.gov.au

The OCG aims to respond to requests as soon as practicable and will advise the person if the request is likely to require more time to process. An OCG staff member will contact the person to advise them of the outcome of the request.

What happens if we do not provide you with information?

The OCG may sometimes decide not to provide access to personal information in response to the request. We will confirm this with the person in writing and will indicate our reasons.

If a person is not satisfied with our response or they think we are taking an unreasonable amount of time to respond to their request, they have the right to seek an internal review by the OCG. However, before seeking an internal review about the latter, we encourage the applicant to contact our office to ask for an update or timeframe (see Options for seeking review below).

Access to information under the GIPA Act

A person may also request access to information held by the OCG under the *Government Information (Public Access) Act 2009* (GIPA Act). A person may seek access to their own personal or health information, as well as information which contains personal information about another person.

A written application for access to information under the GIPA Act requires the payment of an application fee of $30. The GIPA Act also requires the OCG to notify the person of its decision and provide reasons for its decision about whether or not to provide access to the information.

Information about how to make an application under the GIPA Act (including the GIPA application form) and payment of the fee can be found on the OCG's website at: https://ocg.nsw.gov.au/about-us/access-information.

An application to access information should be sent to the General Counsel Directorate at Legal@ocg.nsw.gov.au

If an applicant is not satisfied with our decision made on an access application under the GIPA Act, or they are concerned about the release of their personal information, they may seek review of this decision. This may include internal review, or an external review by the Information and Privacy Commission or NCAT.

Amendment of personal or health information

A person can request the OCG to amend or to alter the personal and health information we hold about them.

The right to request amendment is under the IPP in section 15 of the PPIP Act and the HPP in clause 8 of Schedule 1 to the HRIP Act to request the OCG to amend personal and health information we hold about them.

A request to the OCG to alter personal information is usually made where the person needs to update their contact details, such as a change of residential address. A person might also request amendment where they do not agree with the information we hold about them.

The request to amend personal information can involve correction (for example, correcting the spelling of a person's name), addition (for example, where a person requests a note of further information be attached to a file), or deletion (for example, where a person wants the OCG to remove entirely an incorrect record).

The following table outlines where to address a request to amend personal or health information.

Table 3. Where to request an amendment of personal or health information

Information type	Contact
Case-related	If you are seeking amendment in relation to a matter in which you are personally involved, you can contact the business unit or staff member handling the matter (for example, WWCC Directorate, Reportable Conduct Directorate).
Staff records	If you are an OCG staff member, you can contact the OCG's People and Culture team. **Note:** OCG staff can use the SAP system to amend their own personal details (for example, contact details, bank details), without the need for a request.
Other enquiries	OCG's main enquiry line (Ph: 02 8210 3600) or email ocg@ocg.nsw.gov.au

The request should include the following details:

- the applicant's name and contact details, including postal address, telephone number and email address
- indicate whether the request is made under the PPIP Act (personal information) or HRIP Act (health information)
- describe and identify personal or health information the applicant wants to amend and how they wish the OCG to amend it.

We aim to correct inaccurate information such as personal details as quickly as possible. Where we consider more complex requests, we will aim to make appropriate amendments in a timely manner. We will inform the person making the request if the amendment is likely to take longer than expected.

If the OCG is not prepared to amend the personal information in accordance with the request, the person may provide a statement and request the OCG to attach the statement to the information so that it is read with the information. The PPIP Act requires the OCG to take reasonable steps to attach the statement in a manner that is capable of being read with that information.

Options for seeking review

General privacy complaints to the OCG

If a person is concerned about the way the OCG has dealt with or managed their personal or health information, or has concerns about the way the OCG handles information generally, they can raise these matters with the OCG's Director, Corporate Services. See '**Contact details**' for methods of communication, including complaints made in writing or verbally.

We will treat these concerns as complaints unless the person's communication with us indicates a request for internal review (see below). However, if the person would prefer to resolve their privacy concern informally, we encourage them to let us know when they contact us. We may, with the person's consent, suggest we deal with the complaint informally and without the need for an internal review. This will likely occur if we can take action to resolve the complaint easily and quickly and this would be accepted by the person.

A privacy complaint may also be concerned with the handling of personal information generally and would apply to other people's personal information. In that case, the complaint is not likely to be conduct for which we would conduct an internal review.

General privacy complaints may not always be concerned with our conduct against the IPPs or PPIP Act for which there are review rights, including internal review by the OCG or external review by the NCAT. However, we will not limit a person's right to apply for internal review of our conduct and we will discuss this option with them where the complaint appears to be concerned with their personal information.

If a person is not satisfied with the outcome of our response to their complaint, they may still request an internal review by the OCG. Before seeking an internal review, we encourage the person to first discuss any concerns with us.

Internal review of the OCG's conduct under the PPIP Act

An internal review is a review by the OCG of its conduct under the IPPs of the HPPs. A person who is aggrieved by our conduct in relation to their personal or health information may apply for internal review. However, a person cannot ask the OCG to review conduct in relation to another person's personal or health information.

The internal review process is set out under Part 5 of the PPIP Act. It requires both the applicant for review, and the OCG as the agency, to do certain things required by the section 53 of the PPIP Act.

Application requirements

Section 53 requires a person to apply for review of the OCG's conduct in writing. Our internal review must determine whether we think our conduct breached the IPPs or the HPPs.

A person can request an internal review by sending a written application to the OCG Privacy Officer by email at Legal@ocg.nsw.gov.au. See '**Contact details**' for alternative methods of communication.

Section 53 requires that an application for internal review must be made within 6 months from when the applicant first became aware of the alleged breach. However, in some circumstances, the OCG Privacy Officer may consider requests made outside that time, depending on the circumstances.

We consider all written complaints we receive about personal or health information to be a possible application for internal review, even if the applicant does not use the words 'internal review' to describe their written complaint or refer to the PPIP Act of the IPPs.

Where it may not be clear that the applicant is concerned with particular conduct, the OCG will, wherever possible, attempt to ask the applicant to confirm whether they have made a general

complaint or a request for internal review. If the applicant is not sure or does not clarify this, we will likely treat it as an application for internal review.

The request should include:

- the applicant's name and contact details (address, telephone number, email address)
- the specific conduct the applicant is complaining about, and what the applicant alleges the OCG did
- the date when the conduct allegedly occurred
- the date when the applicant first became aware of the conduct
- if the request is lodged outside the 6 month period, an explanation for the late request.

Conduct of the internal review by the OCG

To ensure the integrity and impartiality of the internal review, an officer within the OCG who is independent of the conduct or subject matter of the review is tasked with conducting the review. Generally, the OCG's General Counsel Directorate is responsible for conducting the internal review.

The OCG's process for internal review follows the Privacy Commissioner's guidance, including, IPC's Privacy Internal Review Checklist (available on the IPC's website) and consider any relevant material that the applicant provides to us.

The OCG aims to:

- acknowledge receipt of an application for internal review within 5 working days, and
- complete an internal review as soon as practicable, noting that if it is not complete within 60 calendar days of receiving the request, a person can seek review by the NCAT.

The officer conducting the internal review will inform the applicant of the progress of the internal review, particularly if it is likely to take longer than first expected. The officer will respond to the applicant in writing within 14 calendar days of completing the internal review, as required under section 53(8) of the PPIP Act.

The PPIP Act requires us to inform the Privacy Commissioner of the internal review, the progress and findings of the draft review, and action we propose to take in response to the review. Any submissions made by the Privacy Commissioner to us will be taken into consideration when finalising the review.

At the conclusion of an internal review, the OCG is allowed to do one or more of the following (as set out in section 53(7) of the PPIP Act):

(a) take no further action on the matter
(b) make a formal apology to the applicant
(c) take remedial action (for example, payment of monetary compensation to the applicant)
(d) provide an undertaking that the conduct will not occur again
(e) implement administrative measures to ensure that the conduct will not occur again for example, implement a new training module, change a security setting on a database).

Administrative review by the NCAT

The NCAT can review the conduct which is the subject of the internal review. However, the NCAT does not review our findings in relation to a general privacy complaint.

If an applicant is not satisfied with the finding of an internal review or with the actions we have taken in relation to the internal review under the PPIPA Act, they have the right to seek administrative review by the NCAT.

A person must apply in writing to the NCAT within 28 calendar days from the date of being notified of the findings in the internal review.

A person may also apply to the Tribunal for Administrative Review if we have not completed the internal review within 60 days from the day on which we received the application for internal review.

The key features of the NCAT's review include:

- A person must first seek internal review by the OCG before they have the right to seek review by the NCAT.
- If a person has applied for NCAT review following 60 days since applying for review, the NCAT may make an order for the OCG to complete the internal review.
- An administrative review by the NCAT means the NCAT can review the conduct that was the subject of the internal review.
- The applicant and the OCG may attend mediation by the NCAT to resolve the matter.
- The NCAT may take no action or may make orders requiring the OCG to do certain things.

The NCAT has the power to make orders, including requiring the OCG to:

- refrain from conduct or action that breaches an IPP or HPP
- perform an IPP or HPP
- take steps to remedy any loss or damage suffered by the applicant
- pay compensation.

Information about how to apply for NCAT review, including forms and fees, can be found on the NCAT's website (www.ncat.nsw.gov.au).

Complaints to the Privacy Commissioner

A person can make a privacy complaint about the OCG to the Privacy Commissioner.

The Privacy Commissioner can investigate the complaint and resolve the matter by way of conciliation (see, Contact details, below).

A privacy complaint is treated differently to an internal review. However, the Privacy Commissioner may refuse to deal with a complaint if it would be more appropriate for the complainant to make an application for internal review to the OCG under section 53 of the PPIP Act.

If the OCG is subject to a privacy complaint, the Privacy Commissioner has powers to require the OCG to produce any information to assist the investigation, including, any documents or witness statements.

Contact details

NSW Office of the Children's Guardian

The OCG's General Counsel is responsible for maintaining this PMP. For any questions about this PMP, or our obligations under NSW privacy laws, please contact Legal@ocg.nsw.gov.au or contact our office using the contact details below:

Phone:	(02) 8219 3600
Website:	www.ocg.nsw.gov.au
Email:	ocg@ocg.nsw.gov.au
Post:	Locked Bag 5100, Strawberry Hills NSW 2012

Written complaints about the OCG's management of personal and/or health information can be emailed to ocg@ocg.nsw.gov.au or posted to:

Director Corporate Services
Office of the Children's Guardian
Locked Bag 5100
STRAWBERRY HILLS NSW 2012

Verbal complaints may be made by phoning the OCG Reception on (02) 8219 3600.

Information and Privacy Commission NSW (IPC)

Additional information about rights and obligations under NSW privacy laws is available from the NSW Information and Privacy Commission. A privacy complaint to the Privacy Commissioner may also be made here.

Phone:	1800 472 679
Website:	www.ipc.nsw.gov.au
Address:	Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000
Post:	GPO Box 7011, Sydney NSW 2001

NSW Civil and Administrative Tribunal (NCAT)

Additional information about how to lodge an application for external review is available from NCAT.

Phone:	1300 006 228
Website:	www.ncat.nsw.gov.au
Address:	John Maddison Tower, 86-90 Goulburn Street Sydney
Post:	PO Box K1026, Haymarket NSW 1240

Appendix A: Definitions

The key terms used in this PMP are set out in the table below. The definitions of personal information and health information are also further explained throughout this plan.

Table 4. Definitions

Access to information	Means the ways that a person can ask for access to their personal information using either section 14 of the *Privacy and Personal Information Protection Act 1998* or the *Government Information (Public Access) Act 2009.* A person whose details are included on a register under the *Children's Guardian Act 2019* may also request access to their personal information in addition to section 14 of the *Privacy and Personal Information Protection Act 1998*.
Alteration or amendment of information	Means the ways that a person can make a request for alteration of their personal information under the *Privacy and Personal Information Protection Act 1998* or amendment of their health information under the *Health Information and Privacy Act 2002.*
Authorised representative	Means a person authorised by section 8 of the *Health Records and Information Privacy Act 2002* to do any act on behalf of a person who lacks capacity to consent or to do anything under that Act. (See also "**support person**")
Business unit	A work unit performing a discrete business function within the OCG. Business units within the OCG include: • Compliance • Corporate Services • General Counsel Directorate • NDIS Worker Check • OOHC Directorate • Policy • Reportable Conduct Directorate • Specialised Substitute Residential Care Team • Working with Children Check Directorate.
CG Act	Means the *Children's Guardian Act 2019*.
Chapter 16A	Means Chapter 16A of *the Children and Young Persons (Care and Protection) Act 1998*.

Child/children	When we refer to a child or children, we mean a person who is under the age of 18 years. The *Privacy and Information Protection Act 1998* permits the OCG to collect personal information from a parent or guardian that relates to a person under the age of 16 years.
Children's Guardian/Office of the Children's Guardian	The Children's Guardian
Collection (of personal and health information)	The way in which the OCG acquires personal or health information, which can include by way of a telephone conversation, a voice recording, or when a person provides proof of identity
Disclosure (of personal and health information)	The OCG discloses personal or health information when we make this information known to an individual which was not previously known to them.
Excluded information	Is defined by the *Government Information (Public Access) Act 2009* to mean any information relating to reportable conduct matters in Part 4 of the *Children's Guardian Act 2019* (including report handling, investigative and reporting functions), and any functions of the Children's Guardian relating to Official Community Visitors appointed under the *Children's Guardian Act 2019*).
GIPA Act	Means the *Government Information (Public Access) Act 2009*.
Health information	Defined by the *Health Records and Information Privacy Act 2002* as information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided or to be provided to a person; See the definition at section 6 HRIP Act
Health Privacy Principles (HPPs)	Means the principles set out in Schedule 1 to the *Health Records and Information Privacy Act 2002* (HRIP Act). These 15 HPPs direct the way in which NSW public sector agencies must collect, store, use and disclose a person's health information.
Information held / holds information	Personal information is held by the OCG if: (a) The OCG is in possession or control of the information, or (b) The information is in the possession or control of a person employed or engaged by the OCG in the course of such employment or engagement, or (c) The information is contained in a State record in respect of which the OCG is responsible under the *State Records Act 1998*.
Information sharing and data sharing	Means the disclosure or exchange of information between the OCG and other agencies or third parties, which may be permitted by a formal information or data sharing

	agreement and must be in line with relevant information and privacy laws.
Information Protection Principles (IPPs)	Means the principles set out in sections 8 to 19 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act). These 12 IPPs direct the way in which a NSW public sector agency must collect, store, use or disclose personal information.
Internal review	This is a review by the OCG of its conduct under the PPIP Act, including conduct which breaches an information protection principle. Section 53 requires the OCG to notify the applicant to the review of the findings and any actions to be taken.
NCAT	Is the NSW Civil and Administrative Tribunal. The NCAT conducts administrative review of an agency's conduct under the *Privacy and Personal Information Protection Act 1998*. The NCAT will decide if the conduct breaches an IPP or other provision of the PPIP Act and can take action for a breach by making orders, including, the payment of compensation up to $40,000. In any review, the Privacy Commissioner has the right to appear and be heard, such as making submissions on the conduct under review and the IPPs.
Personal information	Defined by the *Privacy and Personal Information Protection Act 1998* as – information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, including such things as an individual's fingerprints, retina prints, body samples, or genetic characteristics. Health information is excluded from this definition. Other exclusions to the definition of are listed under s4(3) (see the definition at section 4 PPIP Act and section 4(3) PPIP Act and section 5 of the HRIP Act)
Privacy Commissioner	Is the Commissioner appointed under the *Privacy and Personal Information Protection Act 1998* and given a broad range of powers to assist agencies to comply with NSW privacy laws, including issuing guidance. The Privacy Commissioner also has powers to investigate privacy complaints against agencies. The OCG must notify the Commissioner of an application for internal review as the Commissioner can make submissions on the review.
Privacy complaint	This means any complaint about privacy, including where a person raises general concerns about how the OCG deals with personal information or any OCG record systems. A privacy complaint is different from an internal review (see, "**internal review**"). A privacy complaint can also be lodged with the Privacy Commissioner.

Privacy management plan	Means the plan under the *Privacy and Personal Information Protection Act 1998* that explains: • the OCG's policies and practices for complying with the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002* • how the OCG makes its staff aware of these policies and practices • the procedures for dealing with privacy internal reviews • other matters relating to the protection of the personal and health information.
Privacy notice and consent	A privacy notice is distinct from obtaining consent. When we give a privacy notice we tell a person why we are collecting their information and what we are going to do with the personal information. When we obtain consent, we are asking the person to respond and to give their consent to do particular things with the information.
Privacy officer	The OCG Privacy Officer is General Counsel and is assisted in this function by staff in the General Counsel Directorate.
Privacy obligations	We use this term to describe the IPPs and HPPs and any exemptions to those principles that apply to the OCG.
Public register	A register of personal information that is required by law to be, or is made, publicly available or open to public inspection, whether or not upon payment of a fee. Personal information in a public register includes health information as defined by the *Health Records and Information Privacy Act 2002*.
Public sector official	We use this term from the definition in the *Privacy and Personal Information Protection Act 1998* to mean a person who is employed or engaged by the OCG as a public sector agency. We also use the term "public official" when referring to the *Public Interests Disclosure Act 2022* to include a person who is employed by the OCG or who is engaged under a contract of service to provide a service for the OCG.
Publicly available information	We use this term to refer to the information for which the OCG is required to make publicly available. The OCG is authorised to make any government information it holds publicly available unless there is an overriding public interest against disclosure.
Reportable conduct scheme	This requires heads of relevant entities to notify reportable allegations (allegations that constitute sexual offences, sexual misconduct, physical assault, neglect, ill-treatment and behaviour that causes psychological harm to children) or reportable convictions (a conviction for an offence

	involving reportable conduct) against its employees. The role of the OCG is to review an entity's response to allegations against employees and to handle complaints about the investigation process. We may require the relevant entity to provide further information in relation to the reportable allegation or conviction, or the entity's response. We may also investigate an allegation, or an entity's handling of an allegation, if we hold significant concerns about a situation.
Staff	When we use this term, we refer to any person working in a casual, temporary, or permanent capacity in the OCG, including consultants and contractors.
Support person	We use this term to mean a person who supports or cares for an individual and is recognised by that individual as their authorised support person. This may not necessarily be a formal or legal arrangement, but it permits us to deal with that individual when we have obtained consent from the individual to authorise the collection of information from the other person.
WWC Act	Means the *Child Protection (Working with Children) Act 2012.*
Working with Children Check Unit	Means that part of the Office of the Children's Guardian that exercises functions in relation to working with children check clearances under the *Child Protection (Working with Children) Act 2012*.

Appendix B: Examples of information we hold and how we manage this information (OCG functions)

This section explains the key functions of the Children's Guardian and the activities of the OCG's business units to show the types of personal information they are required to collect under our legislation and how they manage this personal information.

Working With Children Check (WWCC)

The Working with Children Check function is exercised by the Children's Guardian in line with the *Child Protection (Working with Children) Act 2012* (WWC Act) and the *Child Protection (Working with Children) Regulation 2013 (WWC Regulation)*. The WWC Act requires people who engage in paid or volunteer child-related work to hold a WWCC clearance or have a current WWCC application, unless an exemption applies. It also requires employers, unless exempted, to require child-related workers to hold a WWCC clearance or a current WWCC application, and to verify and record clearance details of those workers.

The WWCC Directorate collects information from individuals applying for, or renewing, a WWCC for the purpose of determining a WWCC application or an assessment of an applicant or the holder of a clearance. This is through an online application form which requires the person to input their personal information. When a person applies for, or renews a WWCC, we require them to prove their identity.

The privacy collection notice to the online of application form informs applicants about the collection, use and disclosure of their personal information for the purpose of their WWCC application or WWCC clearance. For example, our notice advises that:

- the personal information collected will be provided to the Australian Criminal Intelligence Commission (ACIC) for the purpose of a National Police History Check.
- the OCG may obtain and disclose information to other organisations for the purpose of assessing the WWCC application.
- the purpose of collecting identity verification information and information-sharing of this information between the OCG, Transport for NSW and Service NSW.
- the OCG will inform notifiable persons (for example, the applicant's employer) if the applicant is interim barred or barred from working in child-related work.
- the applicant will not be able to hold a WWCC clearance where the applicant does not consent to provide their personal information in line with the online application form and as required by law.
- any information that was used to assess their WWCC application may be made available to a tribunal or court in relation to a review of the decision by the OCG to refuse their application to work with children or to cancel their clearance to work with children.

During the assessment of an applicant for a WWCC clearance or a holder of a clearance, we collect information directly from the applicant/holder. This may include, a range of formal documents, such as, statutory declarations, personal and professional references, and expert reports. Other information may be provided verbally from the applicant which the OCG officer will record in writing in a file note as close in time to when it was collected from the person.
Section 31 of the WWC Act also give the Children's Guardian power to issue a written notice to a person to require that person to provide information that is relevant to an assessment of whether a person poses a risk to the safety of children. The information we collect through these notices includes:

- Law enforcement information (from both NSW and Commonwealth agencies)
- Court records, judgments, sentencing remarks and court transcripts

- Information about the person's involvement with government and non-government agencies, such as child protection services and the Department of Corrective Services
- Medical records and reports
- information about a person's employment.

These types of records include information about the applicant/holder's identity (for example, name, contact details) as well as details about their personal experiences, opinions, medical and mental health history. This information may also contain personal information about other individuals, such as victims/complainants and witnesses (for example, name, contact details, opinions and statements).

We only use this information if it is relevant, up to date and complete for the purpose of determining a WWCC application or an assessment of the holder of a clearance. We may also use this information if the applicant/holder seeks a review of a decision at the NCAT which was advised to the applicant/holder through the privacy notice at completion of the online WWCC application form.

All information collected for the WWCC is stored securely on the **Working with Children Check Register**, for which access is password-protected. Only authorised staff have access to the Register. Hard copy records that are received for the purpose of the WWCC are scanned and saved on the Register and original copies are securely destroyed.

We will only provide information about our assessment of a WWCC application to the person that the application relates to, or to the person who they have authorised to be provided information, such as a legal representative or support person. An applicant/holder must verify their identity (for example. by confirming full name, date of birth) before we will provide information to them. Before we provide information to the person's legal representative or support person, we ask the applicant/holder to first provide a signed authority which permits the OCG to correspond with the representative/support person about the individual's WWCC application.

We are permitted by law to not comply with the IPPs in certain circumstances which may arise in our WWC functions. For example:

- Chapter 16A of the *Children and Young Person's (Care and Protection) Act 1998* allows for personal information to either be received or provided to other government agencies and employers where it relates to the safety, welfare and wellbeing of children and young people.
- Section 36A of the WWC Act permits the Children's Guardian to exchange WWCC information with an interstate screening agency.

We may also be permitted to disclose personal information in legal proceedings where the OCG is a party, for example, where a person applies to the NCAT for administrative review of the OCG's decision to bar or not grant them a WWCC. We use personal and/or health information about the person for the purpose of preparing submissions for those proceedings, and may also collect information, including exercising the Children's Guardian's power to require production of information under section 31 of the WWC Act, or by way of application for a summons to be issued by the NCAT.

The OCG will also disclose the personal and/or health information it holds or collects to its legal representative in proceedings, the Crown Solicitor's Office. Information held or collected by the OCG for the purpose of an applicant/holder's WWCC is provided to the applicant/holder, their legal representative, the NCAT or court, and individuals commissioned to provide expert evidence in the NCAT or court proceedings.

Other WWCC Registers and databases

Under section 37 of the WWC Act, the Children's Guardian is permitted to collect and maintain a database of certain matters. The Children's Guardian currently maintains a database of employers and other persons who verify information about WWCC clearances or applications.

The WWCC Directorate operates how this register is accessed and requires employer and other persons to:

- register to access the database by providing their personal information to allow login access.
- before verifying the status of a clearance or application, employers or other persons must provide the information collected directly from the person the subject of the WWCC application, which includes, the individual's WWCC number, full name and date of birth before they can verify the status of the clearance or application.

The Children's Guardian is required by section 36D of the WWC Act to record information about a negative notice issued to a person on the National Reference System database. This information includes, interim bar, disqualification, refusal of clearance, or cancellation of clearance. The database is secure and only can only be accessed by authorised OCG staff.

Reportable Conduct Scheme

The Reportable Conduct Scheme under Part 4 of the *Children's Guardian Act 2019* (CG Act) is administered by the Children's Guardian with the object to protect children from harm.

The Scheme monitors how organisations covered by the Scheme ("**relevant entities**") investigate and respond to reportable allegations and reportable convictions. The head of a relevant entity is required by law to notify the OCG of reportable allegations and convictions against their employees, investigate the allegation, advise us of the outcome and take appropriate action to prevent reportable conduct by employees.

The head of the relevant entity provides this information to the OCG's Reportable Conduct Directorate (RCD) through an online notification form that is available on the OCG's website, and in interim and finalised entity reports.

The Reportable Conduct Scheme function means the OCG holds very sensitive and personal and health information about persons, including children and young persons.

Permissions given to the Children's Guardian to use and disclose information

The Reportable Conduct Scheme gives certain permissions to the Children's Guardian to use personal information, despite the IPPs and the HPPs.

The RCD uses the information it collects to decide whether to conduct its own investigations, or in conducting preliminary enquiries and investigations. Section 44 of the CG Act states that the use and disclosure IPPs will not apply to the preliminary enquiries made by the Children's Guardian to decide whether to carry out an investigation.

The RCD will also provide feedback to relevant entities regarding the handling of a matter. The RCD also uses the information in making referrals to the OCG's WWCC Directorate which is a requirement of section 56 of the CG Act.

The information collected by the OCG in exercising its functions in the Reportable Conduct Scheme includes:

- information setting out the facts and circumstances of reportable allegations
- information obtained in an investigation, such as interview transcripts of witnesses or victim statements
- summary and analysis of the information
- information about the findings of the investigation, and the action taken in response to the findings.

These include personal or health information about the person who is the subject of the investigation (for example, name, contact details, alleged conduct, personnel records and any opinion about that person). The information collected by the RCD also includes the personal information about other individuals, such as the alleged victim who is a child or other persons

involved in the reportable conduct.

The OCG stores records relating to all notifications of reportable allegations, regardless of the results of the investigation. The records are stored on a secure system called 'Resolve' that is only accessible to authorised staff within the office.

Restrictions on the disclosure of information

The CG Act makes clear that there are limits and even prohibitions on the disclosure of information collected in the exercise of the Reportable Conduct Scheme. Sections 57 and 58 does not permit the Children's Guardian to disclose any information relating to a reportable allegation or reportable conviction, or any information obtained in an investigation or determination into reportable conduct or a reportable conviction, unless certain circumstances apply.

The investigation and reporting records held by the RCD are not publicly accessible as we secure these on databases with password-only access given to designated staff.

Information relating to reportable conduct matters under Part 4 of the CG Act is also protected from public access by legislation. The *Government Information (Public Access) Act 2009* (GIPA Act) treats information of this kind as "excluded information" and contains provisions which allow the OCG to exclude this information from the requirement to give access to a person who makes a GIPA application to the OCG (section 43 of the GIPA Act). If a person in the community makes an application to another agency for information relating to reportable conduct matters (excluded information), the GIPA Act requires that agency to first consult the OCG and obtain the OCG's consent to disclose the information (clause 6 of Schedule 1). Otherwise, that other agency is not permitted to disclose the OCG's excluded information.

The CG Act also contains provisions which have the effect of limiting access to investigation records by requests or subpoenas as evidence in court or tribunal proceedings (section 61 CG Act).

The OCG is required to make certain reports to Parliament under section 138 of the CG Act 2019 which include a description of matters relating to reportable conduct, including trends, investigations and reports. We will not disclose information that would identify an individual, such as naming a person or giving other identifying details.

Children's Employment

The OCG regulates the employment of children under 15 years of age within the entertainment, exhibition, still photography and door-to-door sales industries under the CG Act.

Employers are required to obtain an authority from the OCG to employ children and must comply with the Code of Practice which is produced under the Children's Guardian Regulation 2022. To apply for an authority, employers are required to provide business names, ABN, address, contact name and contact details as well as payment details. This information is obtained directly from the company representative and is stored on a secure database within the OCG network. Access to this information is only available to staff working in the Children's Employment team.

We maintain a register of authorised employers on the OCG website which is updated each Monday. The register only provides the employer's name, trading name, Authority identification number, and start and expiry dates.

We can require the production of information about the employment of children. Under clause 56 of the CG Act, it is a condition of an employer's authority (or exemption to hold an employer's authority) that the employer must give the Children's Guardian information that the Children's Guardian reasonably requires.

We are also provided with the name and date of birth of each child that is employed, to allow us to assess the level of risk the employment may pose on the child and to ensure specific conditions of employment are enforced.

The OCG may disclose an employer's personal information to NSW Police via a referral for further investigation or for the issuing of penalty notices. This information is provided under the exemption

clauses contained in section 23 of the PPIP Act.

Accreditation and Monitoring of Out-of-Home Care

The OCG has responsibility for accrediting and monitoring "**designated agencies**" that provide statutory out-of-homecare (OOHC) to children and young people under the CG Act.

As part of the accreditation and monitoring programs, the OCG may collect personal information about children and young people in statutory OOHC. This information may include their name, date of birth, legal status, medical conditions, behaviours and case plans. The OCG also obtains personal information concerning the Principal Officer of each accredited agency. This information is collected directly from the individual Principal Officer.

Information collected in our exercise of the OOHC function is stored securely on the OCG network and Records Management System. Some identifying information may be destroyed after an accreditation decision is made or it is no longer required.

The Children's Guardian maintains the following two registers under section 85 of the CG Act as part of its OOHC functions under s.128 of the CG Act (these are discussed below):

- a register for carers (the **Carers Register**),
- a register for residential care workers (the **Residential Care Workers Register**).

Section 86 of the CG Act requires the Children's Guardian to provide access to information held on these registers, upon the request of the Secretary of the Department of Communities and Justice, the Minister administering the *Children and Young Persons (Care and Protection) Act 1998*, and the NSW Ombudsman.

Carers Register

A principal function of the OCG under section 128 of the CG Act is to establish and maintain the Carers Register. This is a centralised database for people who have applied to become, or have become, an authorised carer to provide statutory or supported OOHC in NSW.

The Carers Register is integral to how we accredit and monitor agencies that provide OOHC and adoption services ("**designated agencies"**). The Carers Register provides agencies with access to relevant information which they can use to make decisions about carers.

The Carers Register is accessed by a secure, restricted access system designed to improve the authorisation process and support better information sharing between designated agencies. The Carers Register can be accessed through the OCG's website. The Carers Register holds information about:

- carer applicants
- authorised carers
- household members.

The Carers Register stores information about:

- application and authorisation history, including where applications have been refused or a carer's authorisation has been cancelled or suspended
- associations between carers and households, including individual household members, and any movements into and out of households
- any history a prospective carer or their household members has with other designated agencies, including any current associations
- reports which detail households and their application or authorisation history.

The Carers Register records information to identify carer applicants and authorised carers, and their household members, including their names, previous names, gender, date of birth and whether they identify as Aboriginal or Torres Strait Islander.

Information recorded about household member information includes, the residential address, a list of persons living in the home and the outcome of a home inspection. The Carers Register does not record details of children in care at these households.

Designated agencies are required to inform authorised carers/carer applicants and their household members that, by law, their information must be entered onto the Carers Register. While the consent of authorised carers and their household members is not required before the designated agency can enter those details into the Carers Register, designated agencies must inform authorised carers and household members of the information which will be recorded.

We will ensure that information on the Carers Register is not disclosed unless there is lawful excuse (section 86(1) CG Act). We will comply with section 87 of the CG Act in dealing with request for information by a person whose details are included on the Register.

Residential Care Workers Register

The Residential Care Workers Register is a register which requires designated agencies to record all residential care workers before they are able to work with children in statutory or supported out-of-home care. The Residential Care Workers Register is a separate register from the Carer Register, and captures residential care workers, or those providing care in residential care.

The Residential Care Workers Register is a secure, restricted access database which holds information about individuals who have reached the final stages of a recruitment process and those who have been engaged as residential care workers. The Residential Care Workers Register can be accessed through the OCG's website.

The Residential Care Workers Register contains only that information necessary to link a worker to the agencies that have engaged their services and to flag any alerts between those agencies. The following information is held on the Residential Care Workers Register:

- full name (and any other, or previous, names), date of birth, gender (if disclosed)
- if the individual identifies as Aboriginal and/or Torres Strait Islander (if disclosed)
- the date and outcome of mandatory probity checks including:
    - Working with Children Check (including the APP / WWC number and expiry date)
    - Nationwide Criminal Record Check
    - Other Agency Check
    - Community Services Check (to be phased in at a future date)
- the decision to engage or not engage an individual, and once engaged:
    - the commencement and end dates of the individual's engagement,
    - the date of any current reportable allegations and any finalised outcomes (but excluding the details of the allegation which will not be held on the Register).

The residential care worker must provide consent before their information is entered on the Residential Care Workers Register. The agency is responsible for requesting consent. The residential care worker's application will not proceed without giving consent to be entered on the Residential Care Workers Register, and they cannot be considered for employment as a residential care worker. By giving their consent at the application stage, the worker agrees to:

- their details being collected and added to the register as part of the recruitment process
- their personal information being used, or disclosed, by the recruiting agency on an ongoing basis. This includes the exchange of information between agencies where it is related to the safety, welfare and wellbeing of children and young people as permitted by Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*.

We will ensure that information on the Residential Care Workers Register is not disclosed unless there is lawful excuse (section 86(1) CG Act). We will comply with requests for information received from a person whose details are included on the Register, in accordance with section 87 of the CG Act.

Specialised Substitute Residential Care (SSRC) Register

The OCG is responsible for monitoring organisations that provide or supervise SSRC under the CG Act and Children's Guardian Regulation 2022 (CG Regulation). SSRC is an arrangement between a parent and an organisation for a child to receive care away from their usual home for 3 or more nights in any 7-day period. The care must be for respite or behaviour support or funded by the National Disability Insurance Scheme (NDIS).

Organisations that provide SSRC must apply for access to the SSRC Register, which is established by the OCG. The SSRC Register can be accessed through the OCG's website. The SSRC Register is a secure online database that records information (updated by the care provider or supervising designed agency) about children or young people in care and the organisations who provide or supervise that care. Under clause 35 of the CG Regulation, the care provider/agency must record the following personal information on the Register about a child including:

- full name and other names the child is or has been known by
- gender
- date and place of birth
- whether the child is an Aboriginal person or a Torres Strait Islander person
- whether the child has a significant disability.

The SSRC Register is an important tool for the OCG in monitoring the time a child or young person spends in the care of SSRC providers. We use the information on the SSRC Register for the purpose of carrying out our functions, which involves identifying additional supports for the family or in our formalised planning for longer-term placements.

We restrict access to the SSRC so that is only made available to certain individuals and organisations, in accordance with clause 34 of the CG Regulation. We will ensure that information on the Register is not disclosed unless there is lawful excuse (section 86(1) CG Act). We will comply with requests for information received from a person whose details are included on the Register, in accordance with section 87 of the CG Act.

Appendix C: Examples of information we hold and how we manage this information (OCG admin activities)

The following outlines the types of administrative activities which require us to collect personal and health information. We provide a high-level summary of these activities.

Staff

We collect personal information about our staff, including:

- contact details (for example, name, address, telephone number, email address, date of birth)
- demographic information (for example, information about our culturally diverse staff)
- information about staff health or disability adjustments
- attendance and leave records (including bank account and tax file number)
- emergency contact details
- family and care arrangements
- medical conditions and illnesses, medical assessments/records and medical certificates
- work health and safety records (including workers' compensation record).

We collect and use this information for our administrative requirements as an employer, including, leave management, workplace health and safety, and performance management, performance management and evaluation records, information relating to secondary employment, information relating to conflict of interests, redundancy and termination decisions.

We do not ask for more personal information than what is required. We advise staff when collection is voluntary or mandatory and of any possible consequences of not providing it to us. We generally use information with the consent of the person unless an exemption under the PPIP Act or HRIP Act permits us to use information without consent. We may also be permitted to disclose information to a third party, for example, to an insurer for workers' compensation purposes.

Our day-to-day human resource operations are conducted under an outsourced arrangement called GovConnect. GovConnect holds personal information and is responsible for how some personal information is used for recruitment, work arrangements, payroll and leave records. Under the contractual arrangements, GovConnect is bound to comply with the PPIP Act and HRIP Act.

OCG staff members may access, without cost, their own personnel file, or any other related human resources file that contains their personal or health information. Staff have direct access to view their own personal information at any time when using secure personnel systems such as SAP and MyCareer. Staff can access and edit their own personal information on SAP and MyCareer, for example, updating contact details and bank details on SAP.

No one else has authorised access to personnel files apart from staff in the OCG's People and Culture team, nominated GovConnect staff, and other authorised delegates. To carry out their role, OCG staff in managerial roles may hold and have access to the personal information of staff who report to them. This information is held in the SAP and MyCareer systems.

Recruitment

When people apply for jobs at the OCG they send personal information such as their names, contact details and work history. This information is provided (in electronic and hard copy) by the OCG's People and Culture team to the convenor of the panel for the particular position (the convenor of the panel is the contact person stated on the job advertisement). Convenors store this information securely. The convenor only discloses this personal information to other panel members, the OCG's People and Culture team, and to the Children's Guardian.

After recruitment is finalised, the convenor returns all the information back to the OCG's People and

Culture team. Information relating to successful applicants is retained, including for use in talent pool lists. Information contained in unsuccessful applications is destroyed.

Successful applicants are invited to complete various forms to commence their employment with the OCG. See '**Staff**' (above) for the types of information collected. These forms include questions which encourage people to provide certain demographic information that may be sensitive personal information, such as to identify their racial background and cultural information. Applicants are made aware that answering these questions is optional. We collect that information to gather statistics and insights into the wider public sector.

Website and media

The OCG website address is: www.ocg.nsw.gov.au. This website uses Google Analytics to monitor online behaviour and help analyse how users use the site. When you visit our website to read pages or download information, we do not collect any personal information about you.

We use our website to promote the legislation administered by the Children's Guardian, and to publish resources to help our stakeholders who have legal obligations under those laws to understand and comply with those obligations. We also receive public enquiries and feedback through an online form on our website. The information collected via these online forms is sent to secure servers and to our shared drive. This website data is not stored on our website and is not publicly available. We do not publish personal or health information on our website without permission.

Our Media and Communications team deals with media enquiries. We do not provide personal or health information that would identify an individual in our responses to the media without the consent of the person to whom the information relates.

Subscriber, mailing and contact lists

We hold personal contact details in subscriber, mailing, distribution, and contacts lists. That personal information is collected from people who have asked to be included on these lists. Our main lists are:

- our newsletter subscriber lists – to email our newsletter to those who have requested subscription
- community stakeholders list – to contact non-government organisations and other members of the community about our work.

We generally collect names, email addresses and the agency where a person is employed. We do not collect personal information without consent, and we advise people how we will manage their personal information when they provide it to us. We keep our lists separate from each other and use each subscriber list only for the purpose of communication for which we have advised.

We are careful when sending bulk emails to large numbers of subscribers. We do not disclose individual email addresses when sending out bulk emails.

We rely on people providing their accurate personal information to us and we are careful to enter the correct information into our records. Anyone can subscribe or unsubscribe from our newsletter list or contact our office to change their details on other lists. We can delete individual entries on request or if we receive error messages in response to our email communications.

Conferences and other events

We sometimes deliver conferences, seminars and other events to our stakeholders, which may involve other agencies, private organisations and particular parts of the community. We will consider our compliance with the PPIP Act and the HRIP Act when we are organising events and aim to notify people of how we will manage their personal and health information. We usually collect information through registration forms. If we use an event management company to assist with delivering an event, we will make sure that any contracted arrangements include appropriate privacy management practices.

We also participate in community events. We may collect information such as number of visitors to our stall, the kinds of questions asked and what resources we provided. We do not collect personal information such as names and contact details unless someone asks for further assistance from us and we required to later contact that person. We do not give personal information to other agencies or organisations that may have participated in the event. Sometimes we may seek voluntary completion of surveys to help us identify current issues and may also collect different kinds of demographic data which are de-identified. We ensure that any proposed survey or other kind of collection activity is in line with the IPPs.

Training sessions

We deliver training sessions to our stakeholders. We collect registration details of the people who formally sign up to our public events. These details usually require the person's name, email address, and contact numbers. We only use this information to confirm participant numbers and so we can communicate with participants about the event. We may collect sensitive personal information or health information for confirming any dietary requirements, or to provide reasonable adjustments to ensure the accessibility of the training for persons with a disability.

We ask for written feedback from our participants, usually by providing feedback forms or an online survey. These will give the option to be anonymous. We do not ask for names or contact details. We use this feedback to improve our training sessions and material. We may publish collated feedback and comments but do not identify people.

Consultation papers and stakeholder feedback

We will seek feedback from stakeholders and members of the public on our laws by publishing consultation papers. We only ask for information which is helpful to our review and do not unnecessarily seek personal information. We may promote our consultation through other agencies or non-government organisations, as well as using media. We do not require people to participate in the consultation or to provide personal information.

Sometimes people give us feedback on the laws that we administer or other matters about the OCG's functions even where we do not ask for it. They may choose to provide their contact details, or personal opinions, stories, or information about their experiences and backgrounds. They may also give us personal information about other people. We may ask for further personal information but only to clarify the issue being raised.

We store information collected from feedback on our shared drive or in hard copy form. We generally do not disclose personal information.

We may use personal information provided by the person to whom it relates to help us understand the issue being raised and in taking any action to bring issues to the attention of the NSW Parliament or Ministers or public or private sector organisations. If a person has provided the personal information of another person, we will take measures to not disclose the information.

We do not identify a person in our reports or when making submissions publicly available on our website. We may identify a person who has provided consent, or if we notified them in advance of how we would disclose the information they provide to us and they have not let us know of any objections.

Appendix D: Other applicable laws

This section contains information about other laws that concern personal information or privacy. Please note that this is not an exhaustive list of all laws.

Crimes Act 1900 - Under the Crimes Act, OCG staff must not access or interfere with data in computers or other electronic devices unless they are authorised to do so.

Government Information (Information Commissioner) Act 2009 **(GIIC Act)** - Under the GIIC Act, the Information Commissioner has review, investigation and complaint functions which permit the Commissioner to request an agency to provide information. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

Independent Commission Against Corruption Act 1998 (ICAC Act) - Under the ICAC Act, OCG staff must not misuse information obtained in the course of doing their jobs.

Public Interest Disclosure Act 2022 (PID Act) - The PID Act provides OCG employees ("public officials") with the right to make a public interest disclosure about matters such as corrupt conduct, maladministration, waste, and government information contravention in the public sector. The PID Act protects public officials who make disclosures. Only certain persons in the OCG will have access to and deal with public interest disclosures. The definition of personal information under the PPIP Act exempts information about an individual that is contained in a public interest disclosure or that has been collected in an investigation under the PID Act from the definition of "personal information" under the PPIP Act. This means that "personal information" received or collected in the course of an investigation arising out of a public interest disclosure under the PID Act is not subject to the IPPs or HPPs.

State Records Act 1998 and State Records Regulation 2015 - This law sets out the record management responsibilities of public offices in NSW. It also authorises the State Records Authority to oversee record-keeping by public offices in NSW.

Document metadata

Table 5. Document metadata

Details	
Status	Final
Date of approval	May 2024
Approver	NSW Children's Guardian
Compliance level	Mandatory – all staff
Directorate	Corporate Services
Policy owner	Director, Corporate Services
Document location	This plan is available on the OCG website
Next review date	May 2026. The review will be conducted earlier if any legislative, administrative or systemic changes affect how the OCG needs to manage personal and health information.
Superseded document	Privacy Management Plan v2.0 – December 2016
Document reference	A8761201

Office of the Children's Guardian

www.ocg.nsw.gov.au

Switchboard: (02) 8219 3600

Locked Bag 5100
Strawberry Hills NSW 2012