Privacy Management Plan

This plan explains how the Office of the Children's Guardian manages personal and health information in line with the NSW Privacy laws.

Office of the Children's Guardian

Document Title

Policy/Procedure Document Title:	Privacy Management Plan
Summary:	This plan explains how the Office of the Children's Guardian manages personal and health information in line with the NSW Privacy laws.
Status:	Final
Policy/Procedure Number:	32
Version Number:	2.0
File Reference:	
Compliance Level:	Mandatory
Compliance Detail:	All staff
Category:	Governance
Related Policies:	
Superseded Policy Ref:	N/A
Public Availability:	This plan will be made available on the OCG website
Feedback:	Any comments or suggestions can be made to the Director Business and Executive Services
Date Issued:	December 2016
Review Date:	December 2018

Children's Guardian Approval

Kerryn Boland
Children's Guardian

Contents

Introduction

This plan explains how the Office of the Children's Guardian manages personal and health information in line with the NSW Privacy laws.

Why we have a privacy management plan

We have a Privacy Management Plan (plan) because we want our stakeholders and staff to know how we manage personal information. With this plan we also meet our obligations for compliance with S33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

The plan explains how we manage personal information in line with the PPIP Act and health information under the *Health Records and Information Privacy Act 2002* (HRIP Act).

It also explains who a person can contact with questions about the personal or health information we hold, how they can access and amend this information and what to do if they think we may have breached the PPIP Act or the HRIP Act.

We also use this plan to train our staff about how to deal with personal and health information. This helps to ensure that we comply with the PPIP Act and the HRIP Act.

More information about the PPIP Act, the HRIP Act and other privacy–related instruments can be found at Appendix A.

What this plan covers

S33(2) pf the PPIP Act sets out the requirements of this plan. This plan must include:

- Information about how we develop policies and procedures in line with the PPIP Act and the HRIP Act
- How we train staff in these policies and procedures
- Our internal review procedures
- Anything else that we consider relevant to the plan in relation to privacy and the personal and health information we hold.

When we review this plan

We will review this plan every two years. We will review the plan earlier if any legislative, administrative or systemic changes affect how we need to manage personal and health information.

About us

Who we are

The Office of the Children's Guardian is established under the *Children and Young Persons (Care and Protection) Act 1998* as a statutory office.

The Office of the Children's Guardian supports the Children's Guardian in the exercise of her functions. It is an independent public service agency that reports to the Minister for Family and Community Services and to NSW Parliament.

The legislative basis for the work of the Office of the Children's Guardian is contained in the following:

- *Children and Young Persons (Care and Protection) Act 1998*
- *Children and Young Persons (Care and Protection) Regulation 2012*
- *Children and Young Persons (Care and Protection) (Child Employment) Regulation 2010*
- *Child Protection (Working With Children) Act 2012*
- *Child Protection (Working With Children) Regulation 2013*
- *Adoption Act 2000*
- *Adoption Regulation 2013.*

For more detailed information about us and the legal framework applying to our work please refer to our website at www.kidsguardian.nsw.gov.au.

Our functions

Our principal functions are set out in s181 of the *Children and Young Persons (Care and Protection) Act 1998:*

- Exercise functions relating to persons engaged in child-related work, including Working With Children Check clearances, under the *Child Protection (Working with Children) Act 2012.*
- Promote the best interests of all children and young persons in out-of-home care.
- Ensure that the rights of all children and young persons in out-of-home care are safeguarded and promoted.
- Establish a register for the purpose of the authorisation of individuals as authorised carers, and to maintain that register, in accordance with the regulations.
- Accredit designated agencies and to monitor their responsibilities under this Act and the regulations.

- Register organisations that provide or arrange voluntary out-of-home care and to monitor their responsibilities under this Act and the regulations.
- Exercise functions relating to the employment of children, including the making and revocation of exemptions from the requirement to hold an employer's authority.
- Develop and administer a voluntary accreditation scheme for persons working with persons who have committed sexual offences against children.
- Develop and administer a voluntary accreditation scheme for programs for persons who have committed sexual offences against children.
- Encourage organisations to develop their capacity to be safe for children
- Accredit adoption service providers under the *Adoption Act 2000*

Our stakeholders

We may collect personal and health information from our stakeholders in order to do our work, such as:

- Members of the public
- NSW public sector agencies
- Private sector companies
- Solicitors and other legal representatives
- Non-government organisations

How we manage personal and health information

We collect and receive different kinds of personal information in order to conduct our functions.

When we use the term "personal information" we mean it according to the definition in the PPIP Act:

- 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.

In this section, a reference to personal information is also a reference to health information.

Working With Children Check

The Office of the Children's Guardian administers the Working With Children Check (WWCC) under the *Child Protection (Working With Children) Act 2012.*

Information relating to applicants seeking a WWCC is provided by the applicant through the completion of an online application and consent form. When providing consent for a WWCC applicants are also consenting to the OCG obtaining criminal history information as well as information from a variety of sources should the application result in a risk assessment. This information is obtained under Part 5 of

the Child Protection (Working With Children) Act 2012. Personal information that may be obtained includes:

- Criminal History Information relating to persons who apply for a WWCC
- Child Protection information from government and non-government service providers
- Workplace records
- Court records
- Medical information
- Statutory Declarations
- Law enforcement information (NSW and Cth)
- Personal information relating to a person's employment
- Personal references
- Professional references
- Expert reports/opinions
- Legal Advice
- Other information subject to legal professional privilege
- Information about a person's conduct from prescribed or designated agencies shared pursuant to Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*
- Office of the Director of Public Prosecutions
- Information filed as part of Children's, Criminal and Family Court proceedings including judgments, sentencing remarks and court transcripts
- Personal Information provided verbally recorded in contemporaneous file note/record

All information is stored on the secure Working With Children Check System. Hard copy records that are received for the purpose of the WWCC are scanned and saved on the database and original copies are securely destroyed. Only staff who specifically either work or have a management role in relation to the WWCC have access to the database.

We will only discuss or provide information about a WWCC application with the individual that the application relates to. They must provide details of their full name, date of birth and other relevant personal information before information will be provided.

We also receive and collect personal information when an applicant is appealing a decision to bar or not grant a WWCC clearance through the NSW Civil and Administrative Tribunal (NCAT). The OCG is a party to the hearing and the Crown Solicitor acts on behalf of the OCG. Personal information held by the OCG regarding the applicant's WWCC is provided to the applicant, Crown Solicitor and NCAT.

Chapter 16A of the *Children and Young Person's (Care and Protection) Act 1998* also 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.

WWCC Public Register

The OCG is required under Section 37(c) of the *Child Protection (Working With Children) Act 2012* to maintain a database of employers and other persons who verify information about WWCC clearances or applications. Employers must register to access the database by providing sufficient personal information to allow unique login access. Employers or other persons can only verify the status of a clearance or application through the provision of personal information obtained directly from the person who the clearance or application relates to. They must have the individuals WWCC number, full name and date of birth before they can verify the status of the clearance or application.

Section 45 of the *Child Protection (Working With Children) Act 2012* makes it an offence for a person to disclose any information obtained in connection with the exercise of functions under this Act or the regulations unless:

- is made in good faith for the purposes of the exercise of a function under this Act or the regulations, or
- is made with the consent of the person to whom the information relates, or
- is ordered by a court, or any other body or person exercising judicial functions, for the purposes of the hearing or determination by the court, body or person of any matter, or
- is made with other lawful excuse.

Section 45(2) of the *Child Protection (Working With Children) Act 2012* provides that a person who dishonestly obtains confidential information relating to the exercise of functions under this Act or regulations is guilty of an offence.

Children's Employment

The Office of the Children's Guardian regulates the employment of children within the entertainment, exhibition, still photography and door-to-door sales industries under the *Children and Young Persons (Care and Protection) (Child Employment) Regulation 2010.*

Employers are required to obtain an authority from the Office to employ children are required to comply with the Code of Practice. To apply for an authority employers are required to provide personal information such as 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.

The Office of the Children's Guardian is also provided with the name and date of birth of each child that is employed to allow the Office to assess the level of risk the employment may pose on the child and to ensure specific conditions of employment are enforced. Schedule 1 Clause 3 of the *Children and Young Persons (Care and Protection) (Child Employment) Regulation 2015* provides authority to collect this information.

The Office may disclose 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 *Privacy and Personal Information Act 1998.*

Accreditation and Monitoring of Out-Of-Home-Care

The Office of the Children's Guardian has responsibility for accrediting and monitoring designated agencies that provide statutory out-of-home-care (OOHC) to children and young people under the *Children and Young Persons (Care and Protection) Act 1998* and *Children and Young Persons (Care and Protection) Regulation 2012*.

As part of the accreditation and monitoring programs the Office of the Children's Guardian 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, behaviors and case plans. The Office of the Children's Guardian is legally entitled to this information under Section 185 of the *Children and Young Persons (Care and Protection) Act 1998.*

The Office of the Children's Guardian also obtains personal information concerning the Principal Officer of each accredited agency. This information is provided by the individual directly.

Information obtained as part of this function is stored securely of the OCG network or Records Management System. Some identifying information may be destroyed after an accreditation decision is made or it is no longer required.

Occasionally the OCG may need to share information is has obtained for this function with either the Ombudsman or Family and Community Services for child protection purposes. This is done under Chapter 16A of the *Children and Young Person's (Care and Protection) Act 1998* that 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.

Accreditation and Monitoring of Voluntary Out-Of-Home-Care (VOOHC)

The Office of the Children's Guardian has responsibility for regulating the provision of VOOHC under the *Children and Young Persons (Care and Protection) Act 1998* and *Children and Young Persons (Care and Protection) Regulation 2012*. As part of this responsibility the Office has established and maintains a VOOHC Register.

Agencies that provide, arrange or supervise VOOHC must enter every episode of care into the VOOHC Register. The Register is a secure, web-based database hosted by the Government Licensing Service (GLS), and access requires a username and password.

The Register provides VOOHC agencies with access to a child or young person's VOOHC history including any case plans and/or supervision arrangements to ensure that the agency can deliver care that is appropriate and consistent.

Information held for each child or young person includes:

- full name and any previous name
- date and place of birth
- gender
- Aboriginal and Torres Strait Islander status
- disability status
- the name of the agency providing and/or supervising the VOOHC
- length of time spent in VOOHC
- dates of any case plans/reviews.

Section 181 of the *Children and Young Persons (Care and Protection) Act 1998* provides authority to collect this information.

Children and young people and their parents may access and correct information captured on the VOOHC Register by contacting the Office of the Children's Guardian.

Carers Register

A principal function of the Office of the Children's Guardian under Section 181(1)(d) of the *Children and Young Persons (Care and Protection) Act 1998* is to establish a register for the purpose of the authorisation of individuals as authorised carers, and to maintain that register, in accordance with the regulations.

The Carers Register is a secure, restricted access system designed to improve the authorisation process by supporting better information sharing between designated agencies.

The Carers Register holds information about:

- carer applicants
- authorised carers
- household members

The Carers Register records identification information about 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. Recorded household information includes the residential address, a list of persons living in the home and the outcome of a home inspection. Associations between carers and household members are recorded, including movements into (and out of) carer households.

A carers application and authorisation history, including application refusals and any cancellation or suspension of authorisation is recorded on the Carers Register.

The Carers Register shows when a reportable allegation is currently being investigated by an agency, or when the Ombudsman's Office has provided a direction to the agency that the allegations should not be finalised on the Register. In addition, a permanent record of reportable allegations is maintained where a designated agency determiners that they may be ongoing risks that relate to the safety, welfare or wellbeing of a child in out-of-home-care.

Designated agencies are required to inform authorised carers and their household members; and carer applicants and their household members that by law, their information must be entered onto the Carers Register. Consent is nit required from authorised carers and their household members fro their information to be entered into the Carers Register, but designated agencies must inform them of what information will be recorded.

Carer applicant and their household members are not obliged to give consent but their application for authorisation will not proceed without it.

A designated agency only has access to information about its own carers and household members but is able to access any Carers register history of an individual who applies to the agency for authorisation as a carer or becomes a household member.

The Office of the Children's Guardian, Department of Family and Community Services and the NSW Ombudsman have access to the Carers Register information. Law enforcement, investigative and child protection bodies in other jurisdictions may be provided with information from the Carers Register.

Carer applicants, authorised and former carers and their household members can access information about themselves held on the Carers Register including information held about their children.

Child Sex Offender Counsellor Accreditation Scheme (CSOCAS)

The NSW Child Sex Offender Counsellors Accreditation Scheme promotes the well-being of children and young people by establishing a public register of counsellors with the necessary knowledge and skill to work with people who sexually offend against children. The establishment of the Scheme directly relates to our functions under s181(1)(h) of the *Children and Young Persons (Care and Protection) Act 1998*

Counsellors wishing to be listed on this register need to apply for accreditation. Applications are considered by the CSOCAS Panel who will grant accreditation at the appropriate level for a period of up to two years.

All personal information that is available on the public register has been obtained from the individual that it relates to and consent has been obtained for the inclusion of their personal information on the public register available on our website.

Communication and stakeholder engagement

Subscriber, mailing and contacts lists

We keep subscriber, mailing and contacts lists that contain personal information from people who have asked to be included on these lists. We do not generally collect details apart from names, email addresses and agency.

Our main lists that collect personal information are:

- our newsletter scriber list – to email our newsletter to those who have requested subscription
- community stakeholders list – to contact no government organisations and other members of the community about our work

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 them only for the purpose for which we have advised we would use them. 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. Anyone can subscribe or unsubscribe themselves from our newsletter list or contact us to change their details on other lists. We keep these lists as long as they remain current. We can delete individual entries on request or if we receive error messages in response to our communications.

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 include name, email address, contact numbers and agency name (is applicable). We only use this information to confirm numbers and communicate with participants about that particular event.

We only collect health information if a participant has special requirements or adjustments needed for the training.

We ask for feedback from our participants and give them the option of remaining 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 don not identify people.

If someone has an enquiry that we cannot answer straight away we may offer to take down their details so someone can get back to them.

Community Outreach

We participate in community events and visit different communities. We may hold these events or participate in events held by other agencies or organisations.

We may collect very basic information such as number of visitors to our stall and may collect demographic information such as gender, the kinds of questions asked and what resources ww provided. We do not identify individuals. We do not collect personal information such as names and contact details unless someone asks for further assistance from us.

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. We ensure that any proposed survey or other kind of collection complies with the PPIP Act and the HRIP Act.

Conferences and other events

We sometimes deliver or participate in other events including conferences, seminars etc. We will consider the PPIP Act and the HRIP Act when we are organising events and aim to notify affected people how we will manage their personal and health information if we collect it, such as on registration forms.

If we use an event management company to assist with delivering an event we will make sure it has appropriate privacy management practices in place. For more information please refer to our section on private sector companies and contractors.

Website publishing, photography, filming and media

We currently maintain one website www.kidsguardian.nsw.gov.au.

We use our website to promote our Acts and publish resources to help our stakeholders understand and use our Acts. We do not publish personal or health information on our website without permission.

We also collect enquires and feedback through an online form on our website. Our website data is stored on secure servers and on our shared drive.

We may take photos or film events that we hold or participate in and use them for promotional purposes. We will always seek permission of people, including our own staff, before we take photos or film events and advise how we will manage that information. We ask people to sign a consent form. We will respect the wishes of those who do not wish to be photographed or filmed.

We store photos and footage electronically on our shared drive.

Our communications team deals with media enquiries. We do not provide personal or health information to the media in responses without their consent.

Policy development

Feedback and consultation papers

People can give us feedback on the laws that we administer. While we do not ask for it, they may decide to give us personal information such as contact details, personal opinions, stories, 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 may also publish consultation papers to seek feedback on particular aspects of our laws. We do not ask for more information than what is helpful to us. We may promote our consultation through various agency, non-government organisation and media channels, however participation is voluntary.

We store tis information on our shared drive or in hard copy form and generally do not disclose personal information.

We rely on people to give us accurate information and to contact us to amend if necessary.

We use personal information to help us understand the context of the issue being raised and decide whether to write reports or bring issues to the attention of the NSW Parliament or other relevant individuals, Ministers or public or private sector organisations.

When we write reports and make findings or submissions publicly available we do not identify people unless we have already sought the consent of the relevant people or notified them in advance of how we would disclose the information they gave to us.

Staff and contractors

Recruitment

When people apply for jobs at our office they send personal information such as their names, contact details and work history. Our corporate services provider and the business services team gives this information to the relevant convenor of the panel for that particular position (stated on the job advertisement) in electronic or physical files.

The convenor of the panel does not disclose this personal information to anyone in the Office except for business support and to the Children's Guardian. Convenors store this information securely. The convenor does not disclose the information to anyone outside the Office except for the corporate services provider and business services team and other panel members.

After recruitment is finalised convenors give all the information back to the business services team to send to the corporate services provider. They retain information relating to successful applicants and talent pool lists for three years. Unsuccessful applications are destroyed.

Successful applicants are invited to fil out various forms to commence their employment with the Office with further personal information such as bank account details, tax file number, emergency contact details and any disabilities that may impact on their work.

These forms also encourage people to provide sensitive personal information such as racial and cultural information for statistics about the wider public sector. These items are voluntary.

These forms are sent to the corporate services provider and are used for employment purposes such as payroll and setting up personnel files. The business services team keeps copies of this information in secure electronic files.

Staff

At times we collect and manage personal information about our staff such as:

- medical conditions and illnesses
- next of kin
- education
- family and care arrangements
- secondary employment
- conflicts of interest
- pecuniary interests.

We collect this information for various reasons such as leave management, workplace health and safety and to operate with integrity.

We do not ask for more personal information than what is actually required. We advise staff when collection is voluntary or mandatory and of any possible consequences of not providing it to us.

Usually our staff will disclose this information to their direct manager or the business services team. This information may also be provided upward trough relevant reporting lines to the Children's Guardian depending on the situation. The information may also be forwarded to the corporate services provider.

We do not disclose this information to anyone else without consent.

Private sector companies, government agencies and contractors

We may use private sector companies, contractors or even other government agencies to provide services to or for or office. If they will have or are likely to have access to personal information we make sure that thy manage personal and health information in line with the PPIP Act, HRIP Act and information security policies. We might do this by:

- asking for evidence of their information-handling processes
- inserting a privacy clause in all our contracts.

We will also consider how a private sector company or contractor will manage personal or health information we give them before engaging with external providers. We give priority to addressing the issues we identify.

External entities that may manage or collect personal information on our behalf include:

- Infosys and Unisys that provide our human resources and information technology systems and support through an outsourcing agreement
- We use a secure shredding company for the destruction of sensitive documents
- Services NSW collects personal information in relation to the WWCC
- Government Licensing Services hosts the VOOHC and Carers Register
- We procure temporary staff from providers under government contract when necessary
- We may use event management companies to host events and manage registrations
- We may use other independent contractors for various purposes.

Systems and administration

We have a service agreement with Unisys and Infosys to provide our information technology and HR systems and support.

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. Our networks are secure and require individual logins. Our staff do not give out their passwords to anyone or let anyone else use their computer login.

Our information is classified in line with the NSW State Records Keyword AAA Thesaurus.

We aim to comply with State Records legislation. We have in place retention and disposal rules for our general administration and functional information.

We consult with our privacy team when considering and implementing new information management systems and software. We do this to make sure that any new system will comply with the PPIP Act and the HRIP Act. If we are not satisfied with how a system or software will manage personal or health information we give priority to addressing the issues we identify.

Physical security

Our hard copy information is mainly located in our office at 418A Elizabeth Street Surry Hills NSW 2010. We archive older physical files in a secure storage facility in compliance with the *State Records Act 1998*. Our staff have key card access to our office. Visitors cannot enter without our permission and we do not leave visitors unsupervised. Our office is locked outside of business hours.

We keep physical files securely stored when we are not using them. We do not leave sensitive information on the printer and use secure printing where appropriate.

Our staff have unique user accounts and passwords to access our computer systems. Our staff do not give out passwords to anyone or let anyone else use their computer login in accordance with our information security policy.

We use locked bins for sensitive documents that need to be destroyed.

Electronic and physical mail handling

We address outgoing mail and email appropriately and refer incoming correspondence to the correct team or person.

We comply with electronic mail processes.

We record details of all incoming mail and outgoing mail in our electronic document management system.

How to access and amend personal and health information

People have the right to access personal information we hold about them.

They also have the right to amend their own personal or health information we hold, for example if they need to update their contact details.

We must provide access to or amend personal or health information without excessive delay or expense. We do not charge any fees to access or amend personal or health information.

Information request

We encourage people wanting to access or amend their own personal or health information to contact us to request it.

We encourage people to contact the staff member or team managing their information.

Individuals can update their personal WWCC information online or by attending a Services NSW Centre

- Enquiries: contact our main enquiry line or email **kids@kidsguardian.nsw.gov.au**
- Case-related: contact the team or staff member handling the matter
- Newsletter subscriptions: add or remove own details through our website or contact the Communications team
- Staff information: speak with our business services team or contact the HR area of Infosys.

A person does not need to put in a formal request in writing. If necessary we may ask them to verify their identity or make a formal application instead.

We aim to respond to informal requests within 5 working days. We will tell the person how long the request is likely to take particularly if it may take longer than first expected.

We will contact the person to advise them of the outcome of the request. In some cases, particularly if it is sensitive information, we may ask them to make a formal application.

If a person is unhappy with the outcome of an informal request they can make a formal application to us.

Formal application

People also have the right to make a formal application to access or amend personal or health information. A person does not need to ask informally before making a formal application, and a person can make a formal application if they have already asked informally.

A person can make a formal application to the Privacy Contact Officer by email, fax or post (contact details on page 22). The application should:

- Include the person's name and contact details (postal address, telephone number and email address if applicable)
- State whether the person is making the application under the PPIP Act (personal information) or HRIP Act (health information)
- Explain what personal or health information the person wants to access or amend
- Explain how the person wants to access or amend it.

We aim to respond in writing to formal applications within 2 working days. We will contact the person to advise how long the request is likely to take, particularly if it may take longer than expected.

If the person thinks we are taking an unreasonable amount of time to respond to an application, they have the right to seek an internal review. Before seeking an internal review we encourage people o contact our office to ask for an update or timeframe.

Limits on accessing or amending other people's information

We are usually restricted from giving people access to someone else's personal and health information. The PPIP Act and the HRIP Act give people the right to access their own information; they generally do not give people the right to access someone else's information unless authorised by other legislation e.g Subpeona.

Under s26 of the PPIP Act, a person can give us consent to disclose their personal information to someone that would not normally have access to it.

Under s7 and s8 of the HRIP Act an "authorised person" can act on behalf of someone else. The HPPs also contain information about other reasons we may be authorised to disclose health information such

as in the event of a serious and imminent threat to the life, health and safety of the individual, to find a missing person or for compassionate reasons.

If none of the above scenarios are relevant a third party could also consider making an application for access to government information under the GIPA Act.

Review rights and complaints

Internal review by our office

People have the right to seek an internal review under the PPIP Act if they think that we have breached the PPIP Act or HRIP Act relating to their own personal or health information. People cannot seek an internal review for a breach of someone else's privacy, unless they are authorised representatives of the other person.

People must apply for an internal review within six months from when they first become aware of the breach. We may also consider a late application for internal review.

Internal review process

A person can seek an internal review by filling out the internal review form available on our website and sending it to our Privacy Contact Officer by email, fax or post or at our office along with any relevant information.

The Privacy Contact Officer will conduct the internal review unless the internal review is about the conduct of the Privacy Contact Officer. In this case the Children's Guardian will appoint someone else within our office to conduct the internal review.

We aim to:

- Acknowledge receipt of an internal review within five working days
- Complete an internal review within 60 calendar days

The Privacy Contact Officer will inform the person of the progress of the internal review, particularly if it is likely to take longer than first expected.

The Privacy Contact Officer will respond to the person in writing within 14 calendar days of deciding the internal review. This is a requirement under the PPIP Act.

If a person disagrees with the outcome of an internal review or is not notified of an outcome within 60 days they can have the right to seek an external review.

We must notify the Privacy Commissioner of the internal review and of the proposed outcome. The Privacy Commissioner is entitled to make submissions on the subject matter of the application and may undertake the review itself if the Office so requests.

External review by the NSW Civil and Administrative Tribunal (NCAT)

A person can seek an external review if they are unhappy with the outcome of an internal review we have conducted or do not receive an outcome within 60 days.

To seek an external review a person must apply in writing to the NSW Civil and Administrative Tribunal (NCAT). Generally a person has 28 days from the date of the internal review decision to seek an external review. A person must seek an internal review before they have the right to seek an external review.

NCAT has the power to make binding decisions on an external review matter.

For more information about seeking an external review including current forms and fees please contact NCAT:

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

Phone: (02) 9377 5711

Visit/Post Level 9 John Maddison Tower 86-90 Goulburn Street Sydney 2000

The NCAT cannot give legal advice, however the NCAT website has general information about the process it follows and legal representation.

Other ways to resolve privacy concerns

We encourage people to try to resolve privacy issues with us informally before going through the review process, or at least contact the Privacy Contact Officer before lodging an internal review to discuss the issue.

A person can raise their concerns with us by:

- Contacting the Privacy Contact Officer
- Making a complaint directly to the Children's Guardian
- Using our complaint process (available on our website)

A person should remember that they have six months from when they become aware of the potential breach to seek an internal review. This six month time frame continues to apply even is attempts are being made to resolve privacy concerns informally. A person may wish to consider this time frame in deciding whether to make a formal request for an internal review or continue informal resolution.

Promoting the plan

Executive and governance

Our executive team is committed to transparency about how we comply with the PPIP Act and HRIP Act.

Our executive team reinforces transparency and compliance with the PPIP Act and HRIP Act by:

- Endorsing the plan and making it publicly available
- Providing a copy of the plan to relevant oversight bodies such as the Audit and Risk Committee
- Making privacy a standard agenda item in their executive meetings
- Reporting on privacy issues in our annual report in line with the *Annual Reports (Departments) Act 1985* (NSW)
- Confirming support for privacy compliance in the business plans and code of conduct
- Identifying privacy issues when implementing new systems
- Using it as part of our induction for new staff, contractors etc.

Our staff

We make sure that our staff are aware and understand this plan, particularly how it applies to the work that they do. Privacy breaches are more likely to occur when a plan is not sufficiently relevant to the work that is actually done in an agency. With this in mind, we have written this plan in a practical way so that our staff can understand what their privacy obligations are, how to manage personal and health information in their work and what to do if unsure.

We make our staff aware of their privacy obligations by:

- Publishing the plan in a prominent place on our website
- Including the plan as part of induction for new staff and offering training to staff as required
- Providing refresher, specialised and on-the-job privacy training
- Highlighting the plan at least once a year (e.g during Privacy Awareness Week)

When our staff have questions about how to manage personal and health information and this plan does not directly answer them they should consult their manager or the Privacy Contact Officer.

Public awareness

This plan is a guarantee of service to our stakeholders of how we manage personal and health information. Because it is central to how we do business we will make this plan easy to access and easy to understand for people from all kinds of backgrounds. Additionally, we are required to make this plan publicly available as open access information under the GIPA Act.

We promote public awareness of this plan by:

- Writing the plan in plain English
- Publishing the plan in a prominent place on our website
- Providing hard copies of the plan free of charge on request
- Translating the plan into other languages on request or in other formats as required
- Telling people about the plan when we answer questions about how we manager personal and health information.

Contacting us

Privacy Contact Officer

Our Director Legal Services has been given the delegation of Privacy Contact Officer.

The Privacy Contact Officer:

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

Please use the contact details below to contact the Privacy Contact Officer.

Our contact details

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

Website: www.kidsguardian.nsw.gov.au

Email: kids@kidsguardian.nsw.gov.au

Phone: (02) 8219 3601

Mail: Level 13 418A Elizabeth Street Surry Hills NSW 2010

Visit: Level 13 418A Elizabeth Street Surry Hills NSW 2010

Appendix A: about the privacy laws

This section contains a general summary of how we must manage personal and health information under the PPIP Act and the HRIP Act and other relevant laws. For more information please refer directly to the relevant law, visit our website or contact us.

The PPIP Act and personal information

The PPIP Act sets out how we must manager **personal** information.

About personal information

Personnel information is defined in s 4 of the PPIP Act and is essentially any information or opinions about a person whee that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, family life, sexual preferences, financial information, fingerprints and photos.

There are some kids of personal information that are not personal information e.g. information about someone who has been dead for more than 30 years, 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. Health information is generally excluded here as it is covered by the HRIP Act.

Information protection principles

Part 2, Division 1 of the PPIP Act contains 12 IPPS with which we must comply. Here is an overview of them as they apply to us:

Collection

1. We collect personal information only for a lawful purpose that is directly related to our functions and activities.

2. We collect personal information directly from the person concerned.

3. We inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We can tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to us.

4. We ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.

Storage

5. We store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect information from unauthorized access, use or disclosure.

Access and accuracy

6. We are transparent about the personal information we store about people, why we use the information and about the right to access and amen it.

7. We allow people to access their own personal information without unreasonable delay or expense.

8. We allow people to update, correct or amend their personal information where necessary.

9. We make sure personal information is relevant and accurate before using it.

Use

10. We only use personal information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose.

Disclosure

11. We only disclose personal information with people's consent unless they were already informed of the disclosure when we collected the personal information.

12. We do not disclose sensitive personal information without consent e.g ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

Exemption to the IPPs

Part 2 Division 3 of the PPIP Act contains exemptions that may allow us not to comply with IPPs in certain situations. Here are some examples:

- We are not required to comply with IPPs 2-3, 6-8 or 10-12 if we are lawfully authorized or required not to do so.
- We are not required to comply with IPP 2 if the information concerned is collected in relation to a court or tribunal hearing.

We do not use the other exemptions on a regular basis as they are not usually relevant to the work that we do, however if we did use one we aim to be clear about the exemption we have used and our reasons for doing it.

Privacy codes of practice and public interest directions can modify the IPPs for any NSW public sector agency.

There are currently no codes of practice that are likely to affect how we manage personal information.

There are public interest directions that may allow us:

- Not to comply with IPPs 2-3, 6-8, 10-12 if it is necessary in order to properly conduct investigations
- To be exempt from the IPPs when transferring enquiries to another NSW public sector agency
- To disclose personal information to a law enforcement agency

The other public interest directions are unlikely to affect how we manage personal information.

Offences

Offences can be found in s62-68 of the PPIP Act.

It is an offence for us to:

- Intentionally disclose or use personal information accessed in doing our jobs for an unauthorised purpose
- Offer to supply personal information that has been disclosed unlawfully
- Hinder the Privacy Commissioner or a member of staff from doing their job.

Public registers

The PPIP Act also governs how NSW public sector agencies should manage personal information contained in public registers (Part 6 – Public Registers).

Section 57 “Disclosure of personal information contained in public registers” states:

1) The public sector agency responsible for keeping a public register must not disclose any personal information kept in the register unless the agency is satisfied that it is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

2) In order to enable the responsible agency to comply with subsection (1), the agency may require any person who applies to inspect personal information contained in the public register to give

particulars, in the form of a statutory declaration, as to the intended use of any information obtained from the inspection.

Section 58 ‘suppression of personal information” states:

1) A person about whom personal information is contained (or proposed to be contained) in a public register may request the public sector agency responsible for keeping the register to have the information:

   (a) removed from, or not placed on, the register as publicly available, and

   (b) not disclosed to the public.

2) the public sector agency is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, the agency must suppress the information in accordance with the request unless the agency is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information.

3) Any information that is removed from, or not placed on, a public register under this section may be kept on the register for other purposes.

The HRIP Act and health information

The HRIP Act sets out how we manager **health** information.

About health information

Health information is a more specific type of personal information and is defined in s6 of the HRIP Act. Health information can include information about a person’s physical or mental health such as a psychological report, blood test or an X-ray, or even information about a person’s medical appointment. It can also include some personal information that is collected to provide a health service, such as a name and contact number on a medical record.

Health privacy principles (HPPs)

Schedule 1 of the HRIP Act contains 15 HPPs that we must comply with. Here is an overview of them as they apply to us.

Collection

1. We collect health information only for a lawful purpose that is directly related to our functions and activities..
2. We ensure that the health information is relevant, not excessive, accurate and up to date and does not unreasonably intrude into the personal affairs of the individual.
3. We collect health information directly from the person concerned
4. We inform the person why their health information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their health information and any consequences if they decide not to give their health information to us.

Storage

5. We store health information securely, keep it no longer than necessary, and destroy it appropriately. We protect health Information from unauthorised access, use or disclosure.

Access and accuracy

6. We are transparent about the health information we store about people, why we use the information and about the right to access ad amend it.
7. We allow people to access their health information without unreasonable delay or expense.
8. We allow people to update, correct or amend their health information where necessary.
9. We make sure that health information is relevant and accurate before using it.

Use

10. We only use health information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose.

Disclosure

11. We only disclose health information with people's consent unless they were already informed of the disclosure when we collected the health information.

Identifiers and anonymity

12. We do not use unique identifiers for health information as we do not need them to carry out our functions.

13. We allow people to stay anonymous where this is lawful and practicable.

Transfers and linkage

14. We do not usually transfer health information outside New South Wales.
15. We do not currently use a health records linkage system and do not anticipate using one in the future. However is we did, we would not use one without people's consent.

Exemptions to the HPPs

Exemptions are located in Schedule 1 of the HRIP Act and may allow us not to comply with HPPs in certain situations.

An example of an exemption we may sue is that we are not required to comply with HPPs 4-8 and 10 if we are lawfully authorized, required or permitted not to comply with them.

We do not use the other exemptions on a regular basis as they are not usually relevant to the work that we do, however if we do use them we aim to be clear about the exemption we have used ad our reasons for using it.

Heath privacy codes of practice and public interest directions can modify the HPPs for any NSW Public sector agency. There are currently none that are likely to affect how we manage health information.

Offences

Offences can be found in s68-70 of the HRIP Act.

It is an offence for us to:

- Intentionally disclose or use health information accessed in doing our jobs for anything else other than what we are authorised to
- offer to supply health information that has been disclosed unlawfully
- attempt to persuade a person from making or pursuing a request for health information, a complaint to the Privacy Commissioner or an internal review under the PPIP Act.

Other laws that affect how we comply with the IPPs and HPPs

This section contains information about the other laws that affect how we comply with the IPPs and HPPs.

Crimes Act 1900

Under this law we must not access or interfere with data in computers or other electronic devices unless we are authorised to do so.

Government Information (Public Access) Act 2009 (GIPA Act) and Government Information (Public Access) regulation 2009

Under this law peoples can apply for access to government information we hold. Sometimes this information may include personal or health information. If a person has applied for access to someone else's personal or health information we must consult with affected third parties. If we decide to release a third party's personal or health information we must not disclose the information until the third party has had the opportunity to seek a review of our decision.

Independent Commission Against Corruption Act 1998

Under this law we must not misuse information we have obtained in the course of doing our jobs.

Public Interest Disclosure Act 1994 (PICD Act)

Under the PID Act people working within a NSW Public sector agency can make a public interest disclosure to the Information Commissioner about a failure to properly fulfil functions under the GIPA Act.

The definition of personal information under the PPIP Act excludes personal information contained in a public interest disclosure. This means that "personal information" received or collected under the PID Act is not subject to the IPPs or HPPs.

The PID Act requires that we must not disclose information that might identify or tend to identify a person who has made a PID.

State Records Act 1998 and State Records Regulation 2010

This law sets out how we long we must retain and when we can destroy our records. It also authorises the State Records Authority to establish polices, standards and codes to ensure the NSW Public sector agencies manage their records appropriately.

The Office of the Children's Guardian acknowledges that in developing this plan we has borrowed content and layout from the Information and Privacy Commission Privacy Management Plan where that content is of a general nature.