Illawarra Shoalhaven Joint Organisation
Policy Manual

Privacy Management Policy

Contents

1 PURPOSE

The purpose of this Privacy Management Plan (PMP) is to explain how the Illawarra Shoalhaven Joint Organisation (the ISJO) manages personal and health information in accordance with NSW privacy laws.

2 POLICY INTENT

The ISJO is committed to embedding privacy best practice into all business practices and decision making. The ISJO recognises that considering the impact on privacy of any new service, initiative or information system prior to design and implementation is key to this commitment.

Whilst the main objective of this plan is to enshrine best practice in everything we do, the plan also aims to ensure the ISJO's compliance with:

1. Privacy and Personal Information Protection Act 1998 (PPIP Act)
2. Health Records and Information Privacy Act 2002 (HRIP Act).

The ISJO is required to have a PMP under s33 of the PPIP Act which must include:

- information about how the ISJO develops policies and practices in line with State information and privacy legislation
- how the ISJO disseminates these policies and practices within the organisation and trains its staff in their use
- the ISJO's internal review procedures
- anything else the ISJO considers relevant to the Plan in relation to privacy and the personal and health information it holds.

This Plan also explains who you should contact in regard to questions about the information collected and retained by the ISJO, how to access and amend your stored information and what to do if the ISJO may have breached the PPIP or HRIP Acts.

3 POLICY

3.1 What is Personal and Health Information?

Personal information

Personal information is defined in s4 of the PPIP Act as any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name and address, details about their family life, their sexual preferences, financial information, fingerprints and photos.

What is not personal information under the PPIP Act?

There are some kinds of information that are not personal information, these include:

- information about someone who has been dead for more than 30 years
- information about someone that is contained in a publicly available publication
- information or an opinion about a person's suitability for employment as a public sector official.

The Privacy and Personal Information Protection Regulation 2019 also lists other information that is not personal information, such as information about someone that is contained in:

- a document in a library, art gallery or museum
- State records under the control of the NSW State Archives and Records
- public archives (within the meaning of the Copyright Act 1968 (Cth)).

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 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 to a person.

Health information can include, for example, a psychological report, blood test or an x-ray, results from drug and alcohol tests, and information about a person's medical appointments. It can also include some personal information that is collected to provide a health service, such as a name and telephone number.

3.2 Why do we Collect Personal and Health Information?

The ISJO collects personal information in a variety of ways in order to efficiently perform the services and functions we deliver. The ISJO assesses the level of personal information that is appropriate to be collected in relation to each function undertaken with a view to minimising the amount of such information we collect and manage.

Personal and health information may be collected from:

- members of the public
- NSW and Commonwealth public sector agencies
- businesses
- non-government organisations
- employees
- medical professionals.

Contractors acting on the ISJO's behalf may also collect personal information. The ISJO includes clauses in its contracts that require contractors to comply with relevant privacy obligations.

The ISJO has a range of functions involving the collection of personal / health information, including:

- providing services
- consultation with the community, businesses and other stakeholders
- recording, investigating and managing complaints and allegations
- site inspections and audits
- incident management
- enforcing regulations and legislation
- issuing approvals, consents, licences and permits
- providing grant funding

- maintaining the non-residential register of electoral information
- employment practices, including assessing fitness for work.

3.3 How do we Collect Personal and Health Information?

The ISJO collects personal information in a variety of ways including:

- incident reports
- medical assessment reports
- submissions
- application forms
- CCTV footage
- financial transaction records
- contracts
- customer enquiries and correspondence
- web services and smart devices (the Internet of Things)

Unsolicited information

Unsolicited information is personal, or health information provide to the ISJO in circumstances where the ISJO has not asked for or required the information to be provided. Such information is not deemed to have been collected by the ISJO but the access, storage, use and disclosure Information Protection Principles in this Plan will apply to any such information, whilst the ISJO continues to hold this information.

Personal information contained in petitions received in response to a call for submissions or unsolicited petitions tabled at The ISJO meetings will be treated the same as any other submission and may be made available for release to the public.

Personal or health information disclosed publicly and recorded for the purposes of webcasting at ISJO Meetings is not deemed to have been collected by the ISJO. Retention and Use Principles of this information will apply to such information in the ISJO's possession, however Disclosure Principles will not apply as the information was voluntarily disclosed with the prior knowledge that it would be recorded, broadcast via the internet to the public and made available by the ISJO for public viewing.

Privacy Protection Notice

Under s10 of the PPIP Act, when we collect personal information from an individual, such as their name, address, telephone number or email address. The ISJO must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual is made aware of:

- the purposes for which the information is being collected
- the intended recipients of the information
- whether the supply of the information is required by law or is voluntary
- any consequences for the individual if the information (or any part of it) is not provided
- ways the individual can access and correct the information.

Where possible, individuals providing personal information will be given the opportunity to consent to the terms of the provision of the information via a Privacy Protection Notice.

ISJO staff are encouraged to consult with the Privacy Officer ensure that each collection of personal information, and any accompanying Privacy Protection Notice is appropriate and complies with our privacy requirements.

3.4 Personal and Health Information Held by the ISJO

The following is a list of examples of the types of personal and health information and circumstances in which we may collect personal information in exercising the ISJO's functions:

3.5 The ISJO Board

The ISJO holds personal information concerning the ISJO Board such as:

- Personal contact information
- Complaints and disciplinary matters
- Pecuniary interest returns
- Entitlements to fees, expenses and facilities.

3.6 Customers

The ISJO holds personal and health information in its records such as:

- Leases, licences and agreements
- Customer requests
- Financial records
- Donation, grant and sponsorship applications
- Responses to clean up notices regarding health issues
- Submissions and information collected as part of the ISJO's community engagement and consultation activities
- Public access forum applications
- CCTV footage.

3.7 Employees, volunteers and contractors

The ISJO holds personal and health information concerning its employees, volunteers and contractors, such as:

- Personal contact information
- Recruitment material
- Pre-employment medical information
- Bank account details
- Wage and salary entitlements
- Leave and payroll data
- Employee immunisation records and medical certificates
- Volunteers' medical information

- Disclosure of interest returns
- Workers' compensation investigations
- Public interest disclosure investigations
- Performance management plans
- Disciplinary matters.

3.8 How we Manage Personal and Health Information Collected and Held by the ISJO

As outlined elsewhere in this Plan the ISJO collects and manages information from a multitude of sources and will always do so in accordance with the PPIP Act. We also endeavour to make as much information available, to individuals whose information we collect/hold, at the time of collection. Additional information is detailed below for services / functions that frequently collect personal information or manage significant amounts of personal information or data.

Requests for Service, Enquiries and Correspondence

The ISJO receives a significant number of requests for service, as well as general enquiries and correspondence and a certain amount of personal information is required to be collected to allow the ISJO to perform these functions. These requests for service and enquiries are made by people:

- over the phone (The ISJO does not record telephone conversations; however, it does have a voicemail service)
- in writing (e-mail, letter, fax, online form)
- in person at ISJO's office.

The ISJO determines the appropriate level of personal information to be collected for each type of service request and enquiry to allow sufficient information to be an accurate record of the issue and assistance given, but we will not collect unnecessary personal and/or health information.

If the ISJO receives written correspondence, a full copy of whatever is sent is generally kept in the ISJO's electronic document management system. The provision of any personal information is entirely voluntary, and in that respect personal information may be provided that is unsolicited.

Telephone conversations are not electronically recorded. If someone has an enquiry that cannot be answered straight away, the ISJO staff member will offer to take the person's name and telephone number or email address so that another officer of The ISJO can respond.

Complaints and Regulatory Functions

The ISJO receives complaints from members of the public to investigate potential non-compliances with legislation. Most of these investigations are handled in accordance with the relevant legislation governing The ISJO's activities in particular functions.

The ISJO recognises that some people may wish to remain anonymous, however, clear information regarding the consequences of remaining anonymous must be provided. For example, the ISJO may not be able to properly investigate or consider a complaint or review a matter if sufficient information about the matter is not received.

To appropriately investigate most matters, ISJO officers may be required to collect personal information from those parties involved, including names and address, but may also involve detailed correspondence or witness statements for complicated matters.

The ISJO endeavours to maintain the confidentiality of complainants wherever possible, however, at times the ISJO may be required to provide personal information of complainants to other parties due to legislative or court requirements.

Staff and Recruitment

The ISJO collects personal and/or health information from staff members as well as part of our recruitment process. The ISJO will never ask for more personal information than is required for that purpose.

Staff

During the recruitment process and throughout employment, information (including personal and/or health information) is collected from staff members for various reasons, such as leave management, workplace health and safety and to help the ISJO to operate with transparency and integrity. Information collected by the ISJO is retained, to the extent necessary and managed securely. In the exercise of its functions, the ISJO collects and manages personal information about its staff including but not limited to:

- medical conditions and illnesses
- next of kin and contact details
- education
- performance and development information
- family and care arrangements
- secondary employment
- conflicts of interest
- banking details for payroll purposes
- employment history
- details and copies of licences essential to the performance of an officer's role

Recruitment

When people apply for jobs at the ISJO, they send us personal information, including their name, contact details and work history. The ISJO provides this information to the interview panel for that particular position in electronic or hard copy files. The personal information is only used for the purposes of the recruitment process.

After recruitment is complete, successful applicants are required to fill out various forms in order to commence employment at the ISJO. These forms require further personal and health information such as the applicant's bank account details, tax file number, emergency contacts and any disabilities that may impact their work. The information collected is used for employment purposes such as payroll and setting up personnel files and the information is retained in secure storage systems.

Visitors and members of the public (incl. QR Codes)

When consultants, contractors and members of the public visit an ISJO facility they may be required to sign in to the premises. The record of entry maybe recorded in a physical sign-in register or via a digital QR Code check-in process. During periods of health emergencies, such as during a pandemic the ISJO may provide check-in data for a facility to NSW Health, or any other relevant government agency, for the purposes of maintaining and supporting community health and safety. The ISJO may restrict entry or refuse provision of a service if the check-in process is not observed.

Any check-in data collected by the ISJO will be held securely and destroyed on a regular basis in accordance with provisions under the *State Records Act 1998* and the ISJO's Corporate Records Management Policy.

Check-in data collected by the Service NSW QR Code Check-In system will not be held by The ISJO and will be held and stored by Service NSW.

Communications and stakeholder engagement

Subscriber, mailing and contact lists

The ISJO may offer interested stakeholders the opportunity to stay up to date on the activities of the ISJO via subscription to various e-newsletters produced by the ISJO. These services will be on an opt-in basis and personal contact information will be supplied to the ISJO voluntarily by subscribers. No personal information will be collected without consent and those who provide their information will be advised as to how the ISJO will manage it. The information generally collected will include names and email addresses and in some cases areas of interest.

Community engagement and public consultation

The ISJO may undertake public consultation to help guide our decision-making and the provision of services. We may collect information when individuals and organisations participate in such activities. This information may include email addresses and additional demographic information as provided by participants. We may also collect information about usage of our website for consultation purposes such as pages visited, documents downloaded, etc.

We collect this information in order to:

- analyse and interpret it to help meet our objectives and obligations;
- communicate information to you about engagement opportunities, events and other initiatives; and
- respond to enquiries and otherwise engage with stakeholders.

The ISJO Website and Service Providers

The ISJO engages a number of service providers who provide software, website, internet services and computer systems through which the ISJO may collect, store or process your personal information. On occasion our providers may have access to your personal information to facilitate services on behalf of the ISJO. The ISJO ensures that our providers adhere to legislative requirements in relation to Privacy as well as meet the requirements of this Plan.

Cookies

The ISJO uses 'cookie' technology to collect additional website usage data and to improve its services. A cookie is a small piece of text sent to your browser by the ISJO's website. This helps our website to remember viewer preferences and it makes the viewer's next visit easier and the site more useful to the individual. The ISJO uses cookies for the following purposes:

- to better understand how person's interact with our services
- to monitor aggregate usage by our users and web traffic routing on our services
- to improve our services.

Most internet browsers automatically accept cookies. Viewers can restrict that process by editing their browser's options to stop accepting cookies or to generate a prompt before accepting a cookie from websites visited.

Social Media

We use social networking services such as Twitter, Facebook and YouTube in addition to traditional methods, to connect with our audience. These include promoting the ISJO's services and facilities. Our use of social media sites also involves listening to social trends and issues that relate to the ISJO services and events. We use various tools to view public social media and website commentary in which the ISJO's accounts may not necessarily be tagged – and engage directly with members of the public to provide information or a better level of customer service. In doing so, we may temporarily collect and store personal information.

To protect privacy and the privacy of others we advise that individuals not include any personal information including phone numbers and email addresses in such communications.

Any personal information collected by the ISJO will be handled in line with this Plan. The social networking service will also handle personal information for its own purposes. These sites have their own privacy policies and we would recommend that individuals access and read those policies.

The Internet of Things

The Internet of Things (IoT) is a broad term that generally refers to physical devices connected to the internet that collect, share or use data. IoT devices and the data they collect can provide convenience, efficiency and insights into essentially every aspect of our world. For the ISJO, in coming years, the IoT will provide many benefits and has the potential to generate great public value. These large collections of data can, in many cases, constitute personal, health and sensitive information.

Given the passive nature of many IoT devices it can be difficult for individuals to ascertain if their personal information is being collected by an IoT device. For example if "smart bin" technology is introduced it is not possible to have a privacy collection notice on every bin in the city. The ISJO will provide details of what data it collects and what the data will be used for and who it will be shared with, for future IoT devices as they are established. However, this will most likely occur via centralised methods, such as the the ISJO website, rather than at each device or collection point. The ISJO will not use any personal information without permission and will use collated and de-identified data instead.

3.9 Public Registers

Under the PPIP Act a public register is a register of personal information that is required by law to be made, or is made, publicly available or open to public inspection. Enquiries about public registers can be made via The ISJO's website.

Part 6 of the PPIP Act prevents the ISJO employees from disclosing personal information held on public registers, unless the information is to be used for a purpose relating to the purpose of the register.

The ISJO's public registers include but may not be limited to:

Register	**Primary purpose of the Register is to:**
Contracts Register	Identify all contracts over the value of $150,000 entered into by the ISJO
Investments Register	Details of all investments currently held by the ISJO
Record of inspections	Identify any inspections and orders action by the ISJO.

Register of disclosures of interests	Determine whether or not an ISJO official has a pecuniary interest in any matter with which the the ISJO is likely to be concerned. There is a corresponding public accountability purpose and third-party access is a secondary purpose.

Secondary purpose of all public registers

Due to the general emphasis on local government processes and information being open and accountable, it is considered that a secondary purpose for which all public registers are held by the ISJO includes the provision of access to members of the public. Therefore, disclosure of specific records from public registers would normally be considered to be allowable under section 57 of PPIPA.

However, requests for access, copying, or the sale of the whole or a substantial part of a Public Register held by the ISJO will not necessarily fit within this purpose. The ISJO will make an assessment as to the minimum amount of personal information that is required to be disclosed with regard to any request and may seek a statutory declaration to satisfy itself as to the intended use of the information.

Suppression of personal information

Any person whose personal information is recorded in a public register has the right to request that their personal details be suppressed.

The ISJO will comply with the request if it is satisfied the person's safety or wellbeing would be affected by not suppressing the information. Applications to suppress personal details from a public register should be made in writing to the Public Officer.

3.10 How to access and amend personal information

The ISJO ensures that people can access information we hold about them. People have a right to amend their own personal or health information.

How do I access my own personal or health information?

Individuals wanting to access the ISJO's records to confirm or amend their own personal or health information, such as updating contact details can do so by contacting the ISJO either in person or in writing. The ISJO will take steps to verify the identity of the person requesting access to information.

How do I amend my own personal or health information?

Individuals wanting to a amend their own personal or health information must put the request to The ISJO in writing. This application must contain the following information:

- The full name, date of birth and contact details of the person making the request
- State whether the application is under the PPIP Act or HRIP Act
- Explain what personal or health information the person wants to amend
- Confirmation of the applicant's identity.

Accessing or amending other people's personal or health information

The ISJO is restricted from giving individuals access to someone else's personal and health information unless that person provides us with written consent. An "authorised" person must confirm their identification to act on behalf of someone else.

There may be other reasons the ISJO is authorised to disclose personal and 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.

3.11 Data Breaches

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to the ISJO's physical or electronic information or data, such as:

- accidental loss or theft of information or equipment on which such information is stored
- unauthorised use, access to or modification of data or information systems to gain unauthorised access or make unauthorised changes to data or information
- accidental or unauthorised disclosure of personal information (e.g. email containing personal information sent to incorrect recipient)
- personal information published or posted on The ISJO's website without consent
- access to data by an authorised user for unauthorised reasons (e.g. an employee looking up information in a system for personal reasons in breach of the Code of Conduct)
- accidental disclosure of user login details through phishing
- malware infection
- disruption to or denial of IT services.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of personal information.

How we will manage a data breach

The ISJO will be promptly informed of any data breach and will assist in the assessment and management of the breach, including any reporting under NSW's voluntary data breach reporting scheme, in accordance with the Information and Privacy Commission's Voluntary Data Breach Notification guidelines.

The ISJO will determine whether personal information has been accessed and/or disclosed to determine what response should be taken. The ISJO's default position is to voluntarily report data breaches to the Privacy Commissioner.

3.12 Review rights and the complaint process

The ISJO encourages individuals to try to resolve privacy issues with us informally before going through the formal review process to allow speedier resolution of concerns. Any person who may have a privacy concern they can contact The ISJO by phone for advice or for referral to the Privacy Contact Officer. Alternatively write or email the ISJO with any concerns and the ISJO will respond providing advice on the best course of action.

Internal Review

Individuals have the right to seek an internal review under Part 5 of the PPIP Act if they believe that the ISJO has breached the PPIP Act or HRIP Act relating to their own personal and health information. Individuals cannot seek an internal review for a breach of someone else's privacy, unless they are an authorised representative.

An application for internal review must be made to the ISJO in writing within six months of when the affected person first became aware of the conduct or decision that is the subject of the application.

How does the process of Internal Review operate?

The Privacy Contact Officer or their delegate will conduct the internal review. If the internal review is about the conduct of the Privacy Contact Officer, the Executive Officer will appoint another person to conduct the internal

review. The reviewing officer will refer to the Privacy Commissioner's guidance materials when carrying out an internal review.

The ISJO will acknowledge receipt of an internal review within 5 working days and complete an internal review within 60 calendar days.

Once the review is completed, the ISJO may take no further action, or it may do one or more of the following:

- make a formal apology
- take remedial action
- provide undertakings that the conduct will not occur again
- implement administrative measures to reduce the likelihood of the conduct occurring again

Within 14 days of completing an internal review, the ISJO will notify the applicant of the following:

- the findings of the review
- the action proposed to be taken by The ISJO and the reasons for taking that action (if any)
- the right of the applicant to have those findings, and The ISJO's proposed action, administratively reviewed by the NSW Civil and Administrative Tribunal.

The role of the Privacy Commissioner in the review process

The Privacy Commissioner has an oversight role in how privacy complaints are handled and is entitled to make submissions to the ISJO regarding internal reviews. If the ISJO receives an internal review application, it will:

- notify the Privacy Commissioner of the application as soon as practicable
- keep the Privacy Commissioner informed of the progress of the internal review
- inform the Privacy Commissioner of the findings of the review and the action proposed to be taken by The ISJO in relation to the matter.

An individual can also make a complaint directly to the Privacy Commissioner about an alleged breach of their privacy.

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

If the applicant disagrees with the outcome of an internal review or is not notified of an outcome within 60 days, they have the right to seek an external review and may make application to the NSW Civil and Administrative Tribunal (NCAT) for a review of the ISJOs conduct.

An application for external review can only be made after an internal review has been completed and must be made within **28 days** from the date of the internal review decision.

3.13 Promoting Privacy

Compliance strategy

During induction, and on a regular basis, all employees will be made aware of this Plan and it will be made available for on the ISJO's Intranet and he ISJO's website.

ISJO officials will be regularly acquainted with the general provisions of the PPIPA and HRIPA and, in particular, this Plan, the Information Protection Principles, the Public Register provisions, the Privacy Code of Practice for

Local Government, and any other applicable Code of Practice.

Communication Strategy

The ISJO will promote awareness of this plan and rights under PPIPA, HRIPA and this Plan to the ISJO officials by:

- Providing an overview at inductions and including a copy of the plan in induction packs
- Publishing the plan on our internal and external websites
- Offering training sessions on a regular basis as required
- Providing specialised and on-the-job training to key groups
- Promoting the plan regularly though newsletters, all staff emails, online staff forums and initiatives such as Privacy Awareness Week.

Promoting the Plan to the Community

The ISJO promotes public awareness of this Plan to the community by:

- Making it publicly available and publishing it on our website
- Writing the Plan in plain English
- Telling people about the Plan when they enquire about personal and health information
- Provide a link on our website to the Information & Privacy Commission website and distributing copies of literature available on that site
- Including privacy statements on application forms and invitations for community engagement

3.14 Privacy Impact Assessments

The ISJO will endeavour to take a 'privacy by design' approach to ensure compliance with privacy laws. The ISJO will ensure that the privacy impacts of any new project or system development/implementation are thoroughly considered prior to implementation to allow issues of concern or risk to be addressed early in the process.

The ISJO will develop and implement an appropriate process for the assessment of privacy impacts of any new project or system development/implementation. The process will be guided by the NSW Privacy Commissioner's "Guide to Privacy Impact Assessments". A Privacy Impact Assessment shall be conducted whenever personal or health information will be collected, stored, used or disclosed in any project.

4 LEGISLATIVE REQUIREMENTS

This Privacy Management Plan addresses the requirements of the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*. Please refer to "Appendix A" for more information about NSW's privacy laws, the Information Protection Principles and how these directly relate to the activities of The ISJO.

5 REVIEW

This Plan will be reviewed every two years from the date of adoption. It will be reviewed earlier if any legislative or administrative changes affect the ISJO's management of personal / health information.

6 REPORTING

Section 54 of the PPIP Act requires the ISJO, as soon as practicable after receiving an application for an internal privacy review, to notify the NSW Privacy Commissioner of the application, and to keep the Commissioner informed of the progress of the internal review, and inform the findings of the review and of the action proposed to be taken by the ISJO in relation to the matter.

The responsibility for providing such notifications to the NSW Privacy Commissioner lies with the Executive Officer and the ISJO's Privacy Contact Officer.

7 ROLES AND RESPONSIBILITIES

Our Privacy Contact Officer, will be the Responsible Officer for the Policy and will coordinate the following functions in relation to the Policy:

- Maintaining appropriate records relating to the Privacy Management Plan and its application
- Keeping the Plan current, and undertaking regular reviews of both the Plan and associated procedures
- Train and educate relevant employees with respect to the Plan and privacy in general and ensure documents, tools, templates and user guides are current and readily available.
- Provision of advice and ensuring adherence with the Plan and relevant legislation.

Executive Officer

The Executive Officer has the responsibility for appointing an appropriate officer as the ISJO's Privacy Contact Officer to manage the day-to-day activities in relation to the appropriate collections, use and storage of personal and private information of customers and ratepayers.

The Executive Officer will also ensure that an appropriate process is in place for the assessment of privacy impacts of any new project or system development/implementation. The process should be guided by the NSW Privacy Commissioner's "Guide to Privacy Impact Assessments".

Divisional Managers

Divisional Managers are responsible for ensuring their Division adheres to the requirements of this Plan and provide guidance in respect of the importance of protecting the privacy and the personal information of customers and ratepayers collected and held by the ISJO.

Divisional Managers should ensure that the privacy impacts of any new project or system development/implementation are thoroughly considered prior to implementation to allow issues of concern or risk to be addressed early in the process. Divisional Managers are to ensure that any adopted Privacy Impact Assessment process or procedure is followed whenever personal or health information will be collected, stored, used or disclosed in a project.

Staff

Staff shall adhere to the requirements of this Plan and be cognisant of the significant impact that can occur to individuals if their privacy is breached in any way or their personal information is not handled in accordance with this Plan and relevant legislation.

Staff should only access the personal information of a customer or ratepayer if it is a direct requirement of their role and should never release personal or private information to another person without prior approval by their

supervisor. If any doubt exists in relation to any privacy issue, including appropriateness of collecting, using or sharing personal and private information than staff should contact the Privacy Contact Officer immediately for direction.

8 RELATED POLICIES & PROCEDURES

Code of Conduct

9 CONTACT DETAILS

For assistance in understanding the processes under the PPIPA and HRIPA, please contact The ISJO's Privacy Contact Officer or the Information & Privacy Commission.

All communication should be addressed to:

The Privacy Contact Officer

Illawarra Shoalhaven Joint Organisation
Locked Bag 8821, Wollongong DC NSW 2500 Phone: 02 4227 7111
Email: The ISJO@wollongong.nsw.gov.au Website: www.wollongong.nsw.gov.au

Information & Privacy Commission

GPO Box 7011
SYDNEY NSW 2001
Phone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Web: www.ipc.nsw.gov.au

NSW Civil and Administrative Tribunal (NCAT)

Level 10, John Maddison Tower
86-90 Goulburn Street
SYDNEY NSW 2000
Phone 02 9377 5859 Or 1300 006228

APPENDIX A: ABOUT NSW'S PRIVACY LAWS

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

The PPIP Act and personal information

The PPIP Act sets out how the ISJO must manage **personal** information.

About personal information

Personal information is defined in s4 of the PPIP Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name and address, details about their family life, their sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, such as 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 and Health Privacy Principles**

This section contains a general summary of how we must manage personal and health information under the PPIPA and HRIPA and other relevant laws.

PPIPA provides for the protection of personal information by means of 12 Information Protection Principles and HRIPA provides for the protection of health information by means of 15 Health Information Protection Principles.
The ISJO complies with the Information Protection Principles (IPPs) prescribed under PPIPA and Health Privacy Principles (HPPs) prescribed under HRIPA as follows:

- **IPP 1 & HPP 1 Lawful Collection**

The ISJO will only collect personal and/or health information for a lawful purpose as part of its proper functions. The ISJO will not collect any more information than is reasonably necessary to fulfil its proper functions.

Such personal and health information may include names, residential address, phone numbers, email addresses, signatures, medical certificates, photographs and video footage (CCTV).

Anyone engaged by the ISJO as a private contractor or consultant that involves the collection of personal and health information must agree to be bound not to collect personal information by any unlawful means.

Any forms, notices or requests by which personal and health information is collected by The ISJO will be referred to the Privacy Contact Officer prior to adoption or use.

- **IPP 2 & HPP 2 Direct Collection**

Personal information will be collected directly from the individual, unless that person consents

otherwise. Parents or guardians may give consent for minors. Health information will be collected directly from the person concerned, unless it is unreasonable or impracticable to do so.

Collection may occur via phone, written correspondence to the ISJO, email, facsimile, ISJO forms or in person.

The Code makes provision for the ISJO to depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.

The ISJO may collect personal information from other public sector agencies in respect of specific statutory obligations where it is authorised by law to do so.

PIPPA permits non-compliance with this principle if the ISJO is exercising complaint handling, investigative functions or is authorised or required not to comply with the principle under any Act or law.

- **IPP 3 & HPP 3 Requirements when collecting**

The ISJO will inform individuals that their personal information is being collected, why it is being collected and who will be storing and using it. The ISJO will also inform the person how they can view and correct their information.

A Privacy Statement is published on the ISJO's website, intranet, included on forms where personal or health information is collected and available as a handout to the public.

The ISJO will inform persons why health information is being collected about them, what will be done with it and who might see it. The ISJO will also inform the person how they can view and correct their health information and any consequences if they do not provide their information. If health information is collected about a person from someone else, reasonable steps will be taken to ensure that the person has been notified as above.

- **IPP 4 & HPP 4 Relevance of collection**

The ISJO will seek to ensure that personal and health information collected is directly relevant to its functions, is accurate, and is up-to-date and complete. The collection will not be excessive or intrude into the personal affairs of individuals.

The ISJO will in normal circumstances rely on the individual to supply accurate, complete information, although in special circumstances some verification processes may be necessary.

- **IPP 5 & HPP 5 Secure storage**

The ISJO will store personal and health information securely, for no longer than as required by the General Retention and Disposal Authorities for Local Government Records issued by State Records Authority of NSW. It will then be disposed of appropriately. It will be protected from unauthorised access, use or disclosure by application of appropriate access levels to the ISJO's electronic data management system and staff training.

If it is necessary for the information to be given to a person in connection with the provision of a service

to the ISJO (e.g. consultants and contractors), everything reasonably within the power of the ISJO is done to prevent unauthorised use or disclosure of the information.

- **IPP 6 & HPP 6 Transparent access**

The ISJO will provide reasonable detail about what personal and/or health information is stored on an individual.

The ISJO stores information for the purpose of carrying out its services and functions and in order to comply with relevant records keeping legislation.

Individuals have a right to request access to their own information to determine what, if any information is stored, how long it will be stored for and how it is stored (e.g. electronically with open or restricted access to staff, in hard copy in a locked cabinet etc).

Where the ISJO receives an application or request by a person as to whether The ISJO holds information about them, the ISJO will undertake a search of its records to answer the enquiry. The ISJO may ask the applicant to describe what dealings the applicant has had with the ISJO in order to assist the ISJO to conduct the search.

The ISJO will ordinarily provide a response to applications of this kind within 28 days of the application being made.

The ISJO will issue a statement to be included on its website and in its Annual Report concerning the nature of personal information it regularly collects, the purpose for which the personal information is used and an individual's right to access their own personal information.

- **IPP 7 & HPP 7 Access to own information**

The ISJO will ensure individuals are allowed to access their own personal and health information without unreasonable delay or expense.

Compliance with this principle does not allow disclosure of information about other people. If access to information that relates to someone else is sought, the application must be made under the GIPA Act. Where a person makes an application for access under the PPIPA and it is involved or complex, it may be referred, with the written consent of the applicant, as an application under the GIPA Act.

- **IPP 8 & HPP 8 Right to request to alter own information**

The ISJO will, at the request of a person, allow them to make appropriate amendments (i.e. corrections, deletions or additions) to their own personal and health information so as to ensure the information is accurate, relevant to the purpose for which it was collected, up to date and not misleading.

Changes of name, address and other minor amendments require appropriate supporting documentation. Where substantive amendments are involved, an application form will be required, and appropriate evidence must be provided as to why the amendment is needed.

If the ISJO is unable to amend or delete the personal information a statement can be attached in such a manner as to be read with the information.

- **IPP 9 & HPP 9 Accurate use of information collected**

The ISJO will take all reasonable steps necessary to ensure personal and health information is accurate, relevant and up to date before using it.

The ISJO will consider the age of the information, its significance, the likelihood of change and the particular function for which the information was collected.

- **IPP 10 & HPP 10 Limits to use of information collected**

The ISJO will only use personal and health information for the purpose for which it was collected, for a directly related purpose or for a purpose for which a person has given consent. It may also be used without consent in order to deal with a serious and imminent threat to any person's life, health or safety, for the management of a health service, for training, research or to find a missing person.

Additionally, the ISJO may use personal information to exercise complaint handling or investigative functions. The Code makes provision that the ISJO may use personal information for a purpose other than the purpose for which it was created in the following circumstances:

- Where the use is in pursuance of the ISJO's lawful and proper function/s and The ISJO is satisfied that the personal information is reasonably necessary for the exercise of such function/s.
- Where personal information is to be used for the purpose of conferring upon a particular person, an award, prize, benefit or similar form of personal recognition.

- **IPP 11 & HPP 11 Restricted and Limited disclosure of personal and health information**

The ISJO will only disclose personal and health information with the individual's consent or if the individual was told at the time of collection that it would do so. The ISJO may also disclose information if it is for a related purpose and it considers that the individual would not object.

Personal and health information may also be used without the individual's consent in order to deal with a serious and imminent threat to any person's life, health, safety, for the management of a health service, for training, research or to find a missing person.

PPIPA permits non-compliance of this principle if the disclosure is in relation to a complaint that is made to or referred from an investigative agency.

PPIPA permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government (e.g. the Office of Local Government) if the disclosure is for the purposes of informing that Minister about any matter within that administration, or by a public sector agency under the administration of the Premier if the disclosure is for the purpose of informing the Premier about any matter.

- **Special limits on disclosure**

The ISJO will not disclose sensitive personal information without consent unless it is necessary to prevent a serious and imminent threat to the life or health of an individual, in relation to the following:

- Ethnic or racial origin.

- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Health or sexual activities.

The ISJO will not disclose this information to any person or body who is in a jurisdiction outside New South Wales unless:

- A relevant privacy law that applies to the personal information concerned is in force in that jurisdiction.
- The disclosure is permitted under a Privacy Code of Practice.
- The ISJO is requested by a potential employer outside NSW, it may verify that a current or former employee works or has worked for the ISJO, the duration of that work, and the position occupied during that time. This exception shall not permit the ISJO to give an opinion as to that person's suitability for a particular position with any potential employer unless the ISJO is satisfied that the person has provided their consent for The ISJO to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

- **Specific Health Information Privacy Principles**

Health information includes information or an opinion about the physical or mental health or a disability of an individual and includes personal information about:

- A health service provided, or to be provided, to an individual.
- An individual's express wishes about the future provision of health services.
- Information collected in connection with the donation of human tissue.
- Genetic information that is or could be predictive of the health of an individual or their relatives or descendants.

Health information is given a higher level of protection regarding use and disclosure than is other personal information. In addition to the principles, above, the following four additional principles apply specifically to health information:

- **HPP 12 Unique Identifiers**

The ISJO will only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the ISJO to carry out any of its functions efficiently.

- **HPP 13 Anonymity**

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving any health service(s) from the ISJO.

- **HPP 14 Transborder data flow**

The ISJO will not transfer health information out of NSW without the individual's consent unless:

- The ISJO is unable to obtain consent; it is of benefit to the individual and that they would likely give it.
- It is necessary for a contract with a third party.
- To help prevent a serious and imminent threat to life, health or safety of individuals.
- It is permitted by an Act or other law.
- The recipient is subject to protection laws similar to the HRIPA.

- **HPP 15 Cross-organisational linkages**

The ISJO does not participate in a system to link health records across more than one organisation at this time.

If the ISJO decided to use a system like this in the future, the ISJO would make sure that the individual to whom the health information relates expressly consents to the link.

How the Privacy Code of Practice for Local Government affects the Information Protection Principles

With regard to IPPs 2, 3, 10 and 11, the Code makes provision for The ISJO to depart from these principles where the collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.

With regard to IPP 10, in addition to the above, the Code makes provision that The ISJO may use personal information for a purpose other than the purpose for which it was collected where the use is in pursuance of The ISJO's lawful and proper function/s and The ISJO is satisfied that the personal information is reasonably necessary for the exercise of such function/s.

With regard to IPP 11, in addition to the above, the Code makes provision for The ISJO to depart from this principle in the circumstances described below:

1 The ISJO may disclose personal information to public sector agencies or public utilities on condition that:

i The agency has approached The ISJO in writing.

ii The ISJO is satisfied that the information is to be used by that agency for the proper and lawful function/s of that agency, and

iii The ISJO is satisfied that the personal information is reasonably necessary for the exercise of that agency's function/s.

2 Where the ISJO is requested by a potential employer, it may verify that a current or former employee works or has worked for the ISJO, the duration of that work, and the position occupied during that time. This exception shall not permit the ISJO to give an opinion as to that

person's suitability for a particular position with any potential employer unless the ISJO is satisfied that the person has provided their consent for the ISJO to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

Offences

Offences can be found in Part 8 of the HRIP Act. It is an offence for the ISJO to:

- intentionally disclose or use any health information about an individual to which the official has or had access to in the exercise of his or her official functions
- offer to supply health information that has been disclosed unlawfully
- attempt to persuade an individual to refrain from making or to withdraw an application pursuing a request for access to health information or a complaint to the Privacy Commissioner or Tribunal
- by threat, intimidation, or false representation require another person to give consent or to do, without consent, an act for which consent is required.

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

The GIPA Act provides a mechanism to access your personal information or other information. An application can be made to The ISJO to access information that The ISJO holds. Sometimes, this information may include personal and/or health information.

If a person has applied for access to someone else's information, The ISJO will take steps to consult with people who might have concerns regarding disclosure of their personal information. The ISJO will provide notice of the decision to ensure that people who might want to object to the release of information have time to apply for a review of the decision to release information.

State Records Act 1998* and *State Records Regulation 2015

This law sets out when the ISJO can destroy its records. It also authorises the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies, including the ISJO's.