



PRIVACY MANAGEMENT PLAN

Contents

1. Introduction	3
2. Functions of the Commission	3
3. Personal and health information	4
3.1 Key Definitions	4
3.2 Exclusions from the definition of personal and health information	4
4. The IPPs and HPPs	4
4.1 The Information Protection Principles	4
4.2 The Health Privacy Principles	6
5. Types of personal and health information held by the Commission	7
5.1 Employee records	7
5.2 Complaint records	8
5.2.1 Complaint enquiries	9
5.2.2 Valid complaints	9
5.3 JIRS database records - research and sentencing information	10
5.4 Judicial education conferences and events	11
5.5 Surveys	12
5.6 Communications and stakeholder engagement	12
5.7 Visitors and members of the public	13
6. How to access and amend your personal and health information	13
6.1 Formal application	13
7. Privacy breaches and complaints	14
7.1 Requesting an internal review	14
7.2 Internal review process	15
7.3 The role of the NSW Privacy Commissioner for internal reviews	16
7.4 External review process	16
8. Data breach policy	17
9. Promoting the Commission's PMP	17
10. Offences and penalties	18

11. Further information and contacts.....	19
12. Privacy Code of Practice	19

1. Introduction

The Judicial Commission of NSW (the Commission) has developed this Privacy Management Plan (PMP) to explain how the Commission manages personal and health information in accordance with NSW Privacy Laws. This includes the *Privacy and Personal Information Protection Act 1998* (the PPIP Act), the *Health Records and Information and Privacy Act 2002* (the HRIP Act), and the *Government Information (Public Access) Act 2009* (the GIPA Act).

The PMP also explains who you should contact with questions about the information collected and retained by the Commission, how to access and amend your stored information and what to do if you believe the Commission may have breached the PPIP or HRIP Acts.

Additionally, the PMP is used to train Commission staff about how to deal with personal information. This helps to ensure that the Commission complies with the PPIP Act, the HRIP Act and the GIPA Act.

The Commission is required to prepare and implement a PMP in accordance with section 33 of the PPIP Act.

2. Functions of the Commission

The Commission was established in 1987 as an independent statutory corporation under the *Judicial Officers Act 1986* (the Act).

Under the Act, the Commission has three main statutory functions, namely, to:

- provide a continuing education program for the judicial officers of NSW;
- publish information about criminal and civil law, with a focus on sentencing, to assist the courts to achieve consistency in imposing sentences; and
- examine complaints about a judicial officer's ability or behaviour.

The Commission collects, holds, uses and discloses personal and health information for the purpose of carrying out its functions. For instance, the Commission may handle personal and health information for the purpose of complaints handling, recruitment and human resources management.

The Commission takes the privacy of its staff and members of the public seriously and aims to protect the information it collects and holds.

3. Personal and health information

3.1 Key Definitions

- **Collection** – (of personal information) the method by which the Commission acquires personal or health information, which can include a written or online form, a verbal conversation, an online form, a voice recording, or a photograph.
- **Disclosure** – (of personal information) occurs when the Commission provides the information to an individual or body outside of the Commission. This includes the sharing of personal or health information with other public service agencies.
- **Personal information** is 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 (see the definition at s4 PPIP Act and s4(3) PPIP Act and s5 of the HRIP Act).
- **Health information** is any personal information that is information or an opinion about a person's physical or mental health or disability or the provision of health services to them, including an individual's express wishes about the future provision of health services to them (section 6 of the HRIP Act).
- **Privacy principles** – the Information Protection Principles (IPPs) set out in Division 1 of Part 2 of the PPIP Act and Health Privacy Principles (HPPs) set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Within these principles lawful exemptions are provided.
- **Staff** – any person working in a casual, temporary, or permanent capacity in the Commission, including consultants and contractors.

3.2 Exclusions from the definition of personal and health information

Both the Acts exclude from the definition of personal and health information, information which:

- relates to a person who has been dead for more than 30 years; or
- is contained in a publicly available publication; or
- refers to a person's suitability for employment as a public sector official.

4. The IPPs and HPPs

The Commission is guided by the IPPs set out in sections 8 - 19 of the PPIP Act and the HPPs set out in Schedule 1 of the HRIP Act as follows:

4.1 The Information Protection Principles

Collection of information

1. Lawful	The Commission will only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose.
2. Direct	The Commission will only collect personal information directly from the person concerned, unless they have authorized collection from another person, or if the person is under the age of 16 and the information has been provided by a parent or a guardian.
3. Open	The Commission will inform people why their information is being collected, what it will be used for, and to whom it will be disclosed. The Commission will tell people how they can access and amend their personal information and the consequences if they decide not to give it to us.
4. Relevant	The Commission will ensure that the personal information is relevant, accurate, is not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.
Storage	
5. Secure	The Commission will store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.
Access and accuracy	
6. Transparent	The Commission is transparent about the personal information being stored, what it is being used for, and about the right to access and amend it.
7. Accessible	The Commission allows people to access their personal information without excessive delay or expense.
8. Correct	The Commission allows people to update, correct or amend their personal information where necessary.
Use	
9. Accurate	The Commission will ensure that the personal information is relevant, accurate, up to date and complete before using it.
10. Limited	The Commission will only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.
Disclosure	
11. Restricted	The Commission will only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object to the disclosure, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.
12. Sensitive information	The Commission cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

4.2 The Health Privacy Principles

Collection	
1. Lawful	The Commission will only collect health information for a lawful purpose that is directly related to its activities and necessary for that purpose.
2. Relevant	The Commission will ensure health information is relevant, accurate, up-to-date and not excessive and that the collection does not unreasonably intrude into the personal affairs of a person.
3. Direct	The Commission will only collect health information from the person concerned, unless it is unreasonable or impracticable to do so.
4. Open	The Commission will inform a person as to why it is collecting health information, what the Commission will do with it and who else may see it. The Commission will tell the person how they can view and correct their health information and any consequences that will occur if they decide not to provide their information to it. If the Commission collects health information about a person from a third party the Commission must still take reasonable steps to notify the person that this has occurred.
Storage	
5. Secure	The Commission will ensure the health information is stored securely, not kept any longer than necessary and disposed of appropriately. Health information should be protected from unauthorised access, use or disclosure.
Access and accuracy	
6. Transparent	The Commission will explain to the person what health information is being stored, the reasons it is being used and any rights they have to access it.
7. Accessible	The Commission will allow a person to access their health information without unreasonable delay or expense.
8. Correct	The Commission will allow a person to update, correct or amend their personal information where necessary.
9. Accurate	The Commission will ensure that the health information is relevant and accurate before using it.
Use	
10. Limited	The Commission will only use health information for the purpose for which it was collected or for a directly related purpose, which a person would expect, otherwise the Commission would generally need the person's consent to use the health information for a secondary purpose.
Disclosure	
11. Limited	The Commission will only disclose health information for the purpose for which it was collected, or for a directly related purpose that a person would expect, otherwise the Commission would generally need the person's consent.
Identifiers and anonymity	
12. Identifiers	The Commission will only identify people by using unique identifiers if it is reasonably necessary to carry out its functions efficiently.
13. Anonymity	The Commission will give the person the option of receiving services from the Commission anonymously, where this is lawful and practicable.
Transferals and linkage	

14. Controlled transfer	The Commission will only transfer health information outside the State of NSW in accordance with HPP 14.
15. Linkage	<p>The Commission will only use health records linkage systems if the person has provided or expressed their consent.</p> <p>The Commission does not presently use a health records linkage system and does not anticipate using one in the future.</p>

5. Types of personal and health information held by the Commission

The Commission collects and receives people's personal and health information in a variety of ways, in order to undertake its functions.

The collection of this information may be in writing, e-mail, through the Commission's website enquiry form or the Commission's complaint form, over the phone, or in person.

The Commission aims to tell members of the public and its staff members how it will manage their personal information when they seek our assistance; however, under the Commission's function and powers, we do not give people details of personal or health information it receives about third parties unless legally required to do so.

The Commission limits its collection of personal information in relation to the exercise of its functions where appropriate, and ensures that it only collects information where it is reasonably necessary to pursue its legitimate functions and activities. This section contains an outline of the personal information that is collected by the Commission and why the collection is necessary.

This section explains ways in which the Commission collects personal and health information in the course of its functions and powers:

5.1 Employee records

The Commission collects personal and health information from staff members, usually for administrative purposes. Information collected includes, but is not limited to:

- Records of dates of birth, addresses, contact details and emergency contact/next of kin;
- Information required in accordance with recruitment practices (for example, proof of vaccinations and medical certificates as required by the Commission's Leave Policy);
- Payroll, attendance and leave records;
- Copies of passports and/or birth certificates for proof of residency;
- Performance management and evaluation records, and training records;
- Information collected for recruitment purposes, including resumes that are held temporarily and subsequently destroyed;
- Worker's compensation records;

- Records of gender identity, ethnicity and disability for equal opportunity recording purposes; and
- Results of security checks.

In relation to contractors engaged by the Commission, the Commission may also collect personal addresses, phone numbers, bank account details, tax file numbers, ABN and GST details (as necessary).

Employee records prior to 2021 are stored both in hard copy and placed in a locked filing cabinet, which is only accessible to certain Corporate Services - Accounting staff members. Employee records from 2021 onwards are stored in the VisiPay electronic system, which is maintained by the Corporate Services staff members. These records include leave records, payroll processing information, leave accruals, medical certificates and parental leave information. From 2023 onwards, the Commission's Employment Self Service (ESS) Portal has been in operation and staff members have access to the majority of their own personal information, including payslips, leave balances, and superannuation details, which is held in the Commission's Leave Portal. Commission staff also have the ability to change their address details and contact information using the ESS portal.

Employee personnel records for each staff member are also maintained in hard copy and may contain information relating to contractual arrangements and performance development plans. From 2023 onwards, these records are maintained in the Commission's Electronic Documents Records Management System (EDRMS), and is only accessible by certain Corporate Services staff members.

New employees are asked to provide a range of personal information for administrative purposes. Staff are asked to complete Equal Employment Opportunity (EEO) forms upon commencing employment at the Commission. Disability information is collected and used by the Corporate Services team for the purpose of making any necessary adjustments to the workplace. The EEO forms are provided to the Finance Team for the purpose of preparing workforce profile statistics, which must be reported in the Commission's annual reports. Employees' Tax File Numbers are retained on a secure electronic system, VisiPay, which is only accessible by the Finance Team.

payment summaries and ability to change their address details and contact information

Employee records collected by the Commission are retained, to the extent necessary, and managed securely.

5.2 Complaint records

The Commission examines and deals with complaints made against judicial officers under the Act.

5.2.1 Complaint enquiries

The Commission deals with enquiries from members of the public about the complaint process under the Act.

These enquiries are made by members of the public in a variety of ways, including:

- over the phone (the Commission does not record telephone conversations; however, it does have a voicemail service);
- in writing (email, letter, or online form); or
- in person (at the Commission's office or at events held by the Commission).

The Commission decides what level of information is appropriate to be collected for each enquiry on a case-by-case basis, with the understanding that the details collected must contain enough information to be an accurate record of the issue and assistance given, but should not contain unnecessary personal and/or health information.

If someone writes to the Commission, a full copy of whatever has been provided is generally kept by the Commission in its electronic complaints management system. However, if someone calls over the phone and provides a lot of background information, the Commission may decide not to record all the personal information if it is irrelevant to the enquiry.

The Commission recognises that some people may wish to remain anonymous; however, all enquirers are advised that, under the legislation, complaints against a judicial officer cannot be made anonymously.

5.2.2 Valid complaints

The Act requires that a complaint be made in writing and that it name the person who is complaining and the judicial officer being complained about. In order for a complaint to be valid, the particulars of the complaint must be verified by statutory declaration.

The personal and health information dealt with in relation to complaints can include:

- data identifying the complainants and the details from of their complaint;
- data provided by complainants giving the Commission personal and/or health information about other people;
- information obtained in response to the Commission's requests for further information or a request to a judicial officer to provide a response to a complaint;
- information received or collected by the Commission for Conduct Division proceedings, either at the proceedings or from submissions received from the relevant parties; and
- Commission file notes containing personal and/or health information.

Strict confidentiality is observed in relation to data and information relating to complaints. All information relevant to the Commission's complaints function is stored on the Commission's Complaints Database, the Commission's Electronic Record Management System or in hard copy files.

Access to complaints information is limited to the Commission's Chief Executive Officer, Principal Lawyer - Advisory, members of the Commission and the Commission's Conduct Division Panel (if and when constituted). The Commission's Office Coordinator also assists with administrative tasks relating to complaints when necessary. The Commission's electronic systems require multi-factor access authorisation and any hard copy files or papers relating to complaint matters are kept in locked filing cabinets.

Information relating to complaints may not be disclosed by any individuals to any other person without the consent of the person from whom the information was obtained (section 37 of the Act).

5.3 JIRS database records - research and sentencing information

The Commission aims to create valuable resources to improve sentencing efficiency and reduce the number of appeals against sentences which can be used by the judiciary to reduce court delays. The Commission disseminates information through the Judicial Information Research System (JIRS), which is an online database for judicial officers, the courts, the legal profession and government agencies that play a role in the justice system.

Developed by the Commission, JIRS is an extensive, interconnected and hypertext-linked resource that contains case law, legislation, sentencing principles, sentencing statistics and other reference material of use to trial judges. It is our principal means for communicating changes to the criminal law and ensures that judicial officers are kept up to date with the latest developments in law and practice.

The primary legal reference material contained on JIRS includes the full text of judgments from the NSW Court of Criminal Appeal, Supreme Court, Court of Appeal, Land and Environment Court, and Industrial Relations Commission, as well as selected High Court cases. It also includes the full text of NSW and Commonwealth Acts and Regulations.

The secondary legal reference material includes case summaries, commentary on the principles and practice of sentencing, and on-line publications, such as the Judicial Officers' Bulletin. Quantitative reference material is available in the form of comprehensive and dynamic sentencing statistics, which can be located by reference to the sections of relevant legislation.

The main components of the JIRS database, and the information housed on the database includes the following:

- Justice Link case number;
- A link to a summary of the CCA judgment, the judgment (whether it is a Crown appeal or severity appeal) and first instance remarks where available;
- Offence date or start date (where there is a date range);
- Sentence date (first instance or re-sentence date on appeal);
- Offender's characteristics including: number of offences (multiple/one); if a Form 1 was considered; prior record; plea; age and penalty imposed;
- Sentence for the principal offence;
- Aggregate/effective sentence and overall non-parole period where multiple offences; and
- The details for Local and Children's Court matters record a similar range of information concerning an individual offender. They also record whether or not the principal or other offence involve domestic violence, and whether the offender has been charged with any other offences in the particular proceedings.

The Commission's Systems Division is responsible for the ongoing maintenance and development of JIRS.

A database of subscriber details including names, telephone numbers, log-ons, passwords, circuit timetables and information relating to system capacity is stored on an internal network server accessible to Systems staff only and secured by password. The database is used to assist officers with the training of subscribers in the use of the JIRS database. Access to update and correct information is readily provided to individuals on request. All reasonable efforts are made to ensure that the information is up to date before it is used. Judicial officers' passwords and log-on details may also be disclosed to judge's associates on request.

Details relating to log-ons to the JIRS database are recorded by the Systems Division. Records of logons show: who logs on, for how long and which sections of JIRS are viewed. These records are stored in electronic files that are password protected and accessible by only three officers of the Commission; the Chief Executive Officer, the Systems Manager and the Senior Systems Analyst. This logon information is collected to enable the Commission to evaluate usage of JIRS and thereby improve the service provided to users. For example areas of JIRS that record very low usage may be targeted for review or removal. Additionally, subscribers of JIRS who are infrequent users may be approached for training purposes or checked for technical difficulties. The information gathered on usage is disclosed only on a statistical basis in evaluations of JIRS.

5.4 Judicial education conferences and events

When the Commission organises or delivers continuing judicial education for judicial officer, it will collect registration details of those who sign up to these events. The details collected usually include names, titles, email addresses, and contact numbers. Information collected may also contain the personal views and/or opinions of participants. The Commission only collects and uses this information to confirm numbers, tailor the relevant content for the event, and communicate with participants about the event.

The information collected is stored electronically on a restricted folder, in paper form and may be shared with a third-party provider, as necessary.

Health information is only collected if a participant has any special requirements or adjustments needed for the event, and is retained where necessary.

At the conclusion of an event, the Commission will generally ask for feedback from participants, with the option of remaining anonymous. No names or contact details are specifically requested. The Commission uses this feedback to improve its training sessions and materials. The Commission may publish collated feedback and comments but will not identify specific individuals.

5.5 Surveys

The Commission conducts surveys on its research activities, the services provided and its publications.

These surveys may collect different kinds of demographic data, in addition to other personal information such as contact details, personal opinions or views, a judicial officer's experiences in relation to sentencing and other feedback, or background information. The Commission ensures that all surveys or any other kind of collection complies with the PIPP Act and the HRIP Act. The Commission stores this information on its computer network, in an electronic document management system and/or in hard copy files. The Commission does not disclose personal information obtained through surveys, except by consent or as allowed by law.

5.6 Communications and stakeholder engagement

The Commission keeps subscriber, mailing and contact lists that contain personal information from individuals who have asked to be included on these lists. Generally, these lists are associated with the dissemination of information relating to the Commission's publications, such as the Judicial Officers' Bulletin, Bench Books, Journals and other published materials. No personal information is collected without consent, and those who provide their information are advised as to how the Commission will manage it.

The information generally collected will include names, email addresses, and in some cases, agency names and titles.

All subscriber lists are kept separate from each other and each list is used solely for the purpose intended. The Commission does not disclose individual email addresses when sending out bulk emails.

Any individual can choose to unsubscribe from the relevant subscription list or contact the Commission to change their details.

The Commission maintains these subscription lists in a mailing database, known as the Education Directory Interface, and access to the database is restricted to certain staff members of the Publishing Division, and protected by username and password and multi-factor authorisation log-ins.

The Commission does not destroy these subscription lists; they are kept for as long as they are necessary and valid.

5.7 Visitors and members of the public

When members of the public visit the Commission, a log book is used to record the names of people who enter the office beyond the public area. This log book is kept at the reception desk in the Commission's office.

The Commission collects this information for workplace health and safety purposes. The log book is stored in accordance with the Commission's record-keeping procedures.

6. How to access and amend your personal and health information

Everyone has the right to access the personal and/or health information the Commission holds about them. You also have the right to amend your own personal and/or health information which the Commission holds, for example, updating your contact details.

The Commission is required to provide you with access to the personal and/or health information it holds and allow you to amend this information without excessive delay or expense. There is no fee to access or amend your personal and/or health information.

Staff members wanting to access or amend their own personal or health information are encouraged to contact Human Resources.

6.1 Formal application

For members of the public, a request for access to any personal and/or health information held by the Commission should be made in writing to the Commission's Privacy Officer at officeofthecEO@judcom.nsw.gov.au.

Any person can make a formal application to the Commission and this application should:

- Include your name and contact details, including postal address, telephone number and email address;
- explain what you are seeking, such as whether you are enquiring about personal information held about you, or whether you are wishing to access and amend that information;

- if you are seeking to access or amend your own information:
 - explain what personal or health information you want to access or amend; and
 - explain how you want to access or amend it.

The Commission will endeavour to respond to formal applications within 20 business days and will advise an applicant how long the request is likely to take, particularly if it may take longer than expected.

If the Commission decides not to give access or amend your personal or health information, the reason will be clearly explained to you in writing.

You also have the right to make a formal application to access information under the GIPA Act. For more information, please refer to the Commission's 'Access to Information' page here: [Access to information - Judicial Commission of New South Wales \(nsw.gov.au\)](https://www.nsw.gov.au/privacy/your-rights/access-to-information).

7. Privacy breaches and complaints

The Commission is committed to protecting the privacy of personal and health information in accordance with the Privacy Laws.

If you think your privacy has been breached, you can make a complaint in one of the following ways:

- Contact the relevant person/department involved and resolve the matter informally;
- Apply for an internal review; and/or
- Contact the Privacy Commissioner (external review).

7.1 Requesting an internal review

An individual has the right to seek an internal review under the PPIP Act if you believe the Commission has breached the PPIP Act or HRIP Act relating to your personal and/or health information. You cannot seek an internal review for a breach of someone else's privacy unless you are the authorised representative of the other person.

Applications for an internal review must be made in writing and within six months from when you first became aware of the breach.

The Commission encourages individuals to try and resolve privacy issues informally before going through the review process. Individuals are encouraged to contact the Commission's Privacy Officer (details noted at paragraph 11) to discuss any issues before lodging an internal review.

Complaints can be made using the Privacy Complaint Internal Review Application Form (see **Annexure "A"**); however, internal review applications may be lodged in other formats.

7.2 Internal review process

The Commission, after receipt of such an internal review application, will conduct a review to determine:

- whether or not the alleged conduct occurred;
- if so, whether the Commission complied with its privacy obligations;
- if not, whether non-compliance was authorised by an exemption; and/or
- appropriate action (if any) by way of a response and/or remedy.

Once the Commission completes its internal review, the Commission will advise the person aggrieved and the NSW Privacy Commissioner of its findings (if any) and any actions taken as a result of the internal review.

The Commission's Privacy Officer is responsible for receiving, allocating and overseeing internal reviews in relation to privacy matters.

The Commission is required to follow the requirements set out in Part 5 of the PPIP Act when carrying out an internal review, whether the conduct relates to an alleged breach of the PPIP Act or the HRIP Act.

The Privacy Officer will refer to the Privacy Commissioner's guidance materials when carrying out an internal review, in particular ['A guide for conducting internal reviews'](#) and the ['Internal review checklist'](#) available on the NSW Privacy Commissioner's website.

In finalising the internal review, the Privacy Officer will prepare a report containing their findings and recommended actions.

The Commission may:

- take no further action on the matter;
- make a formal apology to the applicant;
- take appropriate remedial action, which may include the payment of monetary compensation to the applicant;
- undertake that the conduct will not occur again; and/or
- implement administrative measures to ensure that the conduct will not occur again.

The Commission will notify the applicant in writing of:

- the findings of the review;
- the reasons for the finding, described in terms of the IPPs and/or the HPPs;
- any action the Commission proposes to take;
- the reasons for the proposed action (or no action); and/or

- their entitlement to have the findings and the reasons for the findings reviewed by the NCAT.

7.3 The role of the NSW Privacy Commissioner for internal reviews

The NSW Privacy Commissioner has an oversight role in the internal review process and may make submissions on internal reviews. In conducting internal reviews about personal or health information, the Commission, in compliance with the Privacy Laws, must:

- Notify the NSW Privacy Commissioner that they have received the application for internal review;
- Keep the NSW Privacy Commissioner informed of the progress of the internal review;
- Consider any relevant material submitted by the applicant or by the NSW Privacy Commissioner;
- Complete the review as soon as possible (and in any case, the Commission must complete the review within 60 days of receipt);
- Once the review is finished, notify the applicant and the NSW Privacy Commissioner of the findings of the review (and the reasons for those findings), and the action proposed to be taken; and/or
- Notify the applicant of their right to have those findings, and the agency's proposed action, reviewed by the New South Wales Civil and Administrative Tribunal (the NCAT).

If the internal review is not completed within 60 days from the date the application was received or that person is dissatisfied with the Commission's findings, then the complainant has 28 days to make an application under section 55 of the PPIP Act to the NCAT for the review of the conduct or decision complained about.

7.4 External review process

If you are unhappy with the outcome of the internal review conducted by the Commission or do not receive an outcome within 60 days, you have the right to seek an external review by the NSW Civil and Administrative Tribunal (NCAT).

You have **28 calendar days** from the date of the internal review decision to seek an external review under Section 53 of the *Administrative Decisions Review Act 1997 (NSW)*.

To request an external review, you must apply directly to the NCAT, which has the power to make binding decisions on an external review. To apply for an external review or to obtain more information about seeking an external review, including current forms and fees, please contact the NCAT:

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

Phone: 1300 006 228

In person: Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW
2000

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

8. Data breach policy

In accordance with section 33(2)(c1) of the PPIP Act, the Commission has implemented a Data Breach Policy, which sets out the procedures and practices used by the Commission to ensure compliance with the obligations and responsibilities set out in Part 6A of the PPIP Act for the mandatory notification of data breach scheme. The Data Breach Policy is available on the Commission's website here: <https://www.judcom.nsw.gov.au/access-to-information/policy-documents/>.

9. Promoting the Commission's PMP

The Commission promotes awareness of the Privacy Laws and the Commission's PMP by:

- Endorsing the PMP by making it publicly available on the Commission's intranet and website. Publication of the PMP on the Commission's website also serves to educate members of the public about their privacy rights in relation to personal and health information held by the Commission;
- Reviewing and updating the PMP every two years;
- Reporting on privacy issues in the Commission's annual reporting in line with the *Annual Reports (Departments) Act 1985 (NSW)*;
- Continuous and ongoing development of information management and cyber security related training;
- Requiring staff members to sign the Commission's Code of Conduct and Confidentiality agreement;
- Highlight and promote privacy related information as part of the Commission staff induction, including the privacy offence provisions;
- Identifying and dealing with privacy issues when implementing new systems, services and processes, and ensuring the Commission's policies comply with privacy legislation;
- Nominating a dedicated Privacy Officer to manage privacy related issues, complaints and/or investigations, and to provide advice on privacy issues as required; and
- Making Commission staff aware of the Commission's privacy obligations by developing training courses and/or materials

10. Offences and penalties

Part 8 of the PPIP Act and the HRIP Act detail various penalties for the offences under the Privacy Laws. The relevant provisions are set out below in the following table:

Legislative provision/s	Details	Maximum penalty
<ul style="list-style-type: none"> Section 62(1) of the PPIP Act Section 68(1) of the HRIP Act 	It is an offence for a public sector official ¹ to corruptly disclose and/or use personal and health information	100 penalty units or imprisonment for 2 years, or both
<ul style="list-style-type: none"> Section 62(2) of the PPIP Act Section 68(2) of the HRIP Act 	It is an offence for any person to induce or attempt to induce a public sector official (by way a bribe or other corrupt conduct) to disclose personal and health information	100 penalty units or imprisonment for 2 years, or both
<ul style="list-style-type: none"> Section 63 of the PPIP Act Section 69 of the HRIP Act 	It is an offence for a person to offer to supply personal or health information that has been disclosed unlawfully.	100 penalty units or imprisonment for 2 years, or both
Section 70(1) of the HRIP Act	<p>It is an offence for a person to (by threat, intimidation or misrepresentation) persuade or attempt to persuade an individual to:</p> <ul style="list-style-type: none"> refrain from making or pursuing a request to access health information; making a complaint to the NSW Privacy Commissioner; making an application for internal review withdraw any such request, application or complaint. 	100 penalty units
Section 68(1) of the PPIP Act	It is an offence for a person to hinder or obstruct any staff member of the NSW Information and Privacy Commission in the exercise of his or her functions under the PPIP Act and/or the HRIP Act.	10 penalty units

¹ A public sector official refers to any person who is employed or engaged by a public sector agency. In this section, it is noted that a public sector official includes a reference to a person who was formerly a public sector official.

In addition to the above offences, section 37 of the Act provides that a member or officer of the Commission or Conduct Division, or a member of a committee of the Commission, shall not disclose any information obtained by the member or officer in the course of his or her office in relation to a complaint, unless the disclosure is made:

- with the consent of the person from whom the information was obtained;
- in connection with the administration or execution of certain provisions of the Act;
- for the purposes of any legal proceedings arising out of this Act or of any report of any such proceedings; or
- with other lawful excuse.

The maximum penalty for this offence is 100 penalty units or imprisonment for one year, or both.

11. Further information and contacts

For further information about the Commission's PMP, or if you have any concerns, please contact the Commission's Privacy Officer using the details below:

Privacy Officer, Judicial Commission of NSW Email: officeofthecpo@judcom.nsw.gov.au Telephone: (02) 9299 4421

For further information on privacy rights and obligations in NSW, please contact the NSW Privacy Commissioner at:

NSW Information and Privacy Commission Telephone: 1800 472 679 Email: ipcinfo@ipc.nsw.gov.au Postal address: GPO Box 7011 Sydney NSW 2001 Street address: Level 17, 201 Elizabeth Street, Sydney 2000
--

12. Privacy Code of Practice

The Privacy Code of Practice for the Judicial Commission of NSW was approved by the Privacy Commissioner on 22 October 2021 – see here for relevant link: [Privacy Codes of Practice \(nsw.gov.au\)](https://www.judcom.nsw.gov.au/privacy/privacy-codes-of-practice) and Annexure "B" for further information.

Version Control

Version	Effective date	Update comments	Author
1.00	1 July 2000	Initial version	Corporate Services
2.00	1 July 2013	Update	Corporate Services
3.00	1 July 2016	Update	Corporate Services
4.00	1 November 2023	Major revision as a result of PPIP Amendment Bill 2022.	Privacy Officer

Publication Information

Title	Privacy Management Plan
Document Type	Policy
Policy Number	
Developer	Privacy Officer
Contact	Privacy Officer
Approver	Chief Executive Officer
Approval date	5 December 2023
Effective date	1 Nov 2023
Review date	This Plan will be reviewed every two years. It will be reviewed earlier if any legislative or administrative changes affect the management of personal and health information by the Commission.



Annexure "A": Privacy Complaint Internal Review Application form

This is an application for review² of conduct under: (please choose one):

- ☐ Section 53 of the *Privacy and Personal Information Protection Act 1998* (PIIP Act)
☐ Section 21 of the *Health Records and Information Privacy Act 2002* (HRIP Act)

1	Name and the address of the agency you are complaining about:	Privacy Officer Judicial Commission of NSW 5/60 Carrington St SYDNEY NSW 2000
2	Your full name:	
3	Your postal address:	
4	Telephone number:	
5	Email address:	
6	If your complaint is on behalf of someone else: a) What is your relationship to this person? b) Is this person capable of making the complaint by himself or herself?	
7	What specific conduct ³ are you complaining about?	

² It is not a requirement under the PIIP Act or the HRIP Act that you complete an application form. This form is designed for your convenience only. However, you must make a written request in some form to the Judicial Commission of NSW for the matter to be a valid internal review.

³ "Conduct" can include an action, a decision, or even inaction by the Judicial Commission of NSW. For example, the "conduct" in your case might be a decision to refuse you access to your personal information, or the action of disclosing your personal information to another person, or the inaction of a failure to protect your personal information from being inappropriately accessed by someone else.

8	<p>Please tick which of the following describes your complaint: (you may tick more than one option)</p>	<input type="checkbox"/> collection of my personal or health information <input type="checkbox"/> security or storage of my personal or health information <input type="checkbox"/> refusal to let me access or find out about my own personal or health information <input type="checkbox"/> accuracy of my personal or health information <input type="checkbox"/> use of my personal or health information <input type="checkbox"/> disclosure of my personal or health information <input type="checkbox"/> other <input type="checkbox"/> unsure
9	<p>When did the conduct occur (date)? (please be as specific as you can)</p>	
10	<p>When did you first become aware of this conduct (date)?</p>	
11	<p>You need to lodge this application within six months of the date at Q10.</p> <p>If more than six months has passed, you will need to ask for special permission to lodge a late application. Please explain why you have taken more than six months to make your complaint: (e.g., I had other urgent priorities – list them, or while the conduct occurred more than six months ago, I only recently became aware of my privacy rights, etc.)</p>	
12	<p>What effect did the conduct have on you?</p>	
13	<p>What effect might the conduct have on you in the future?</p>	

14	What would you like to see the Judicial Commission of NSW do about the conduct? (e.g., an apology, a change in policies or practices, damages paid to you, training for staff, etc).	

I understand that this form will be used by the Judicial Commission of NSW to process my request for an internal review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54(1) of the PPIP Act; or section 21 of the HRIP Act; and that the Privacy Commissioner will be kept advised of the progress of the internal review.

Your signature: _____ Date: _____

Please keep a copy of this form for your records.

For more information on the PPIP Act or the HRIP Act, see: www.privacy.nsw.gov.au.

Annexure “B”: Privacy Code of Practice for the Judicial Commission of NSW (22 October 2021)

JUDICIAL COMMISSION OF NSW CODE OF PRACTICE

This is a code of practice made in accordance with Part 3 Division 1 of the *Privacy and Personal Information Protection Act 1998*.

1. Coverage

This code is intended to cover the Judicial Commission of New South Wales in relation to its activities of monitoring or assist in monitoring sentences imposed by courts, and disseminating information and reports on sentences imposed by courts for the purpose of assisting courts to achieve consistency in imposing sentences.

2. Interpretation

In this code:

“agency” means public sector agency as defined in section 3 of the *Privacy and Personal Information Protection Act 1998*;

“Commission” means the Judicial Commission of New South Wales;

“functions” means functions of the Commission as set out in the section 8 of the *Judicial Officers Act 1986* consisting of monitoring or assist in monitoring sentences imposed by courts, and disseminating information and reports on sentences imposed by courts for the purpose of assisting courts to achieve consistency in imposing sentences;

“information” means personal information as defined in section 4 of the *Privacy and Personal Information Protection Act 1998*;

“section” refers to sections of the *Privacy and Personal Information Protection Act 1998*.

3. The Code

Section 8

There is no intention to depart from the requirements of section 8.

Section 9

Compliance with section 9 is not required if compliance might detrimentally affect or prevent the exercise by the Commission of its functions.

Section 10

Compliance with section 10 is not required if compliance might detrimentally affect or prevent the exercise by the Commission of its functions.

Section 11

There is no intention to depart from the requirements of section 11.

Section 12

There is no intention to depart from the requirements of section 12.

Section 13

Compliance with section 13 is not required if compliance might detrimentally affect or prevent the exercise by the Commission of its functions.

Section 14

Insofar as the Commission is not exempted from the release of information connected with research by the provisions of the *Government Information (Public Access) Act* 2009, this clause enables the Commission to refer requests for information relating to individuals back to the agency from which the information was originally obtained to seek that information.

Section 15

Compliance with section 15(1) and (3) is not required if compliance might detrimentally affect or prevent the exercise by the Commission of its functions.

Section 16

There is no intention to depart from the requirements of section 16.

Section 17

There is no intention to depart from the requirements of section 17.

Section 18

Section 18 does not operate to prevent other agencies from disclosing information to the Commission if, in connection with the Commission's functions, the disclosure is made in response to a request from the Commission for information or by arrangement with the Commission. Section 18 also does not operate to prevent the Commission from providing personal information to judicial officers and courts in connection with its functions.

Section 19

Section 19 does not operate to prevent other agencies from disclosing information to the Commission if, in connection with the Commission's sentencing function, the disclosure is made in response to a request from the Commission for information or by arrangement with the Commission. Section 19 also does not operate to prevent the Commission from providing personal information to judicial officers and courts in connection with its functions.

Public Registers

Part 6 of the *Privacy and Personal Information Protection Act* 1998 does not operate to prevent the Commission from obtaining, in the exercise of its functions, information, including suppressed information, kept on a public register by an agency.