I·C·A·C

INDEPENDENT COMMISSION AGAINST CORRUPTION

NEW SOUTH WALES

NSW INDEPENDENT COMMISSION AGAINST CORRUPTION

# NSW ICAC Privacy Management Plan

December 2023

# Contents

# 1. Introduction

The purpose of this Privacy Management Plan (PMP) is to explain how the NSW Independent Commission Against Corruption ("the ICAC") manages personal and health information in accordance with NSW privacy laws, including the *Privacy and Personal Information Protection Act 1998* ("the PPIP Act") and the *Health Records and Information Privacy Act 2002* ("the HRIP Act").

The PMP explains who to contact with questions about information collected and retained by the ICAC, how individuals can access and amend their stored information and what to do if they believe the Commission has breached the PPIP Act or the HRIP Act.

Section 33 of the PPIP Act requires each public sector agency to have a PMP.
In accordance with s 33(2) of the PPIP Act, the PMP must include provisions relating to:

(a) the devising of policies and practices to ensure compliance by the ICAC with the requirements of the PPIP Act and the HRIP Act, if applicable
(b) the dissemination of those policies and practices to persons within the ICAC
(c) the procedures that the ICAC proposes to provide in relation to internal review under Part 5 of the PPIP Act
(d) the procedures and practices used by the ICAC to ensure compliance with the obligations and responsibilities set out in Part 6A of the PPIP Act for the mandatory notification of data breaches
(e) such other matters as are considered relevant by the ICAC in relation to privacy and the protection of personal information held by it.

This plan was approved by the ICAC's Senior Manager Forum on 1 December 2023 and replaces the ICAC's previous plan, adopted in 2018.

## Reviewing the plan

The ICAC will review this plan every 12 months. The plan will be reviewed earlier if any legislative, administrative or technological changes affect how the ICAC manages personal and health information.

# 2. About the ICAC

The ICAC is a statutory corporation established by the *Independent Commission Against Corruption Act 1988* ("the ICAC Act"). The ICAC's role is to investigate, expose and minimise corruption in and affecting the NSW public sector through investigation, corruption prevention, research and education. It may also investigate certain conduct that may involve possible criminal offences under the *Electoral Act 2017*, the *Electoral Funding Act 2018* or the *Lobbying of Government Officials Act 2011* that the NSW Electoral Commission refers to the ICAC for investigation.

In exercising its functions, the ICAC is required by s 12 of the ICAC Act to regard the protection of the public interest and the prevention of breaches of public trust as its paramount concerns.

In order to fulfil its statutory role, the ICAC may collect personal and health information from its staff, members of the public, public authorities, public officials and private sector companies and organisations.

More detailed information about the role and functions of the ICAC can be obtained by visiting its website at: www.icac.nsw.gov.au.

## 3. The information protection and health privacy principles

The PPIP Act sets out 12 information protection principles, which concern:

- the collection of personal information
- the retention and security of personal information
- steps to be taken to enable a person to ascertain whether an agency holds personal information
- provision of access by a person to that person's personal information
- amending personal information
- ensuring the accuracy of personal information held by an agency
- limits on the use and disclosure of personal information.

Section 27 of the PPIP Act provides that the ICAC is not required to comply with the information protection principles except in connection with the ICAC's exercise of its administrative and educative functions.

Schedule 1 to the HRIP Act sets out 15 health privacy principles. Section 17 of the HRIP Act provides that the HRIP Act does not apply to the ICAC except in connection with its exercise of its administrative and educative functions.

Having regard to s 27 of the PPIP Act and s 17 of the HRIP Act, this PMP deals with the ICAC's compliance with the relevant principles in connection with its administrative and educative functions only.

Section 41 of the PPIP Act and s 62 of the HRIP Act allow the Privacy Commissioner, with the approval of the relevant minister, to make a written direction to waive or modify requirements for an agency to comply with an information protection principle or a health privacy principle. Privacy codes of practice are sometimes made under the PPIP Act or HRIP Act. These can modify the operation of an information protection principle or health privacy principle. Directions and codes of practice are published on the Information and Privacy Commission website at www.ipc.nsw.gov.au**.** There are currently no directions or codes of practice specific to the practices of the ICAC.

# 4. How the ICAC collects and manages personal and health information

In this section, a reference to personal information includes a reference to health information.

The ICAC collects and receives personal information relating to its administrative and educative functions in a number of ways. This includes in writing, by electronic means such as emails, and directly from individuals.

Wherever possible, this information is collected directly from the person concerned. Some information may be collected from third parties, including employment references and information provided as part of the ICAC's security vetting process.

The ICAC will not ask for more personal information than is necessary and makes sure personal information is accurate before using it.

## What is personal and health information?

Section 4 of the PPIP Act and s 5 of the HRIP Act define "personal information" as:

> *Information or an opinion (including information or an opinion forming part of a data base 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.*
>
> *Personal information includes such things as an individual's finger prints, retina prints, body samples or genetic characteristics.*

Under the PPIP Act and the HRIP Act. "personal information" does not include, inter alia, any information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Section 6 of the HRIP Act provides that "health information" includes personal information that is information or an opinion about:

- the physical or mental health or disability of an individual, or
- an individual's express wishes about the future provision of health services to him or her, or
- a health service provided, or to be provided, to an individual.

## Personal information held by the ICAC

The ICAC collects and holds the following personal information in connection with the exercise of its administrative and educative functions:

1. ICAC personnel records, including information held on the ICAC's Human Resources Information Management System, performance management reports, disciplinary files, family care arrangements, secondary employment, banking and taxation records and declarations of conflicts of interest.

2. Medical information provided by ICAC officers for purposes associated with their employment, including applications for leave.
3. Data collected and held on the ICAC's contract database relating to contractors, including consultants, and information such as bank account details, tax file numbers, references and conflicts of interest declarations.
4. Workers' compensation records containing information relating to an injury or illness and other medical information provided by staff.
5. Information relating to the vetting of prospective employees, consultants and contractors including information relating to associates.
6. Data collected and held concerning people attending ICAC training sessions and conferences and/or requesting educational or other resource information, including mailing and contact lists.
7. Images captured by the ICAC's closed circuit television system. The ICAC uses closed circuit television cameras in its foyer for security. A sign at the entrance to the foyer advises that such cameras are in use. Images recorded by the cameras are deleted by being recorded over on a regular basis.
8. Audit logs of when ICAC officers enter and leave ICAC premises. These are recorded for security purposes.
9. Records of names entered in the ICAC hard copy and electronic visitors books. Entries are made of the names of people who enter the ICAC offices beyond the public area. These records are kept for security purposes.

This information is obtained and kept for a number of reasons including various statutory requirements, taxation obligations, audit purposes, payroll facilitation, security, invoice payment, assessment of staff performance, maintenance of statistics and to ascertain staff training needs.

## Storage and security of personal information

Where the above information is held in hard copy format, it is kept in secure storage areas.

Information held electronically is stored on secure password-protected computer databases.

ICAC staff are required to regularly change their passwords and not give out their password to others. The ICAC complies with the NSW Government Cyber Security Policy.

Access to personal information in relation to the ICAC's administrative and educative functions is restricted to those key ICAC officers deemed to require access to that information to perform their functions and to the person to whom the information relates.

Any disclosure of such information is limited to the exercise of functions under the ICAC Act or in compliance with a direction of a Commissioner given under s 111(4)(c) of the ICAC Act, where the Commissioner certifies it is necessary in the public interest to divulge such information.

Hard copy material is mainly located in the ICAC's office on level 7, 255 Elizabeth Street, Sydney. Older files are archived in a secure storage facility. Access to the non-public areas of the ICAC premises is by key-card. Visitors cannot enter these areas

without permission and must be escorted at all times by at least one ICAC officer. Visitors are not granted access to personal information held by the ICAC.

Personal information that is no longer required and can be destroyed is disposed of by either being shredded or placed in locked bins for secure destruction.

The collection, storage, retention and access to personal information held by the ICAC is governed by various ICAC policies set out below.

Parts 8 of the PPIP Act and the HRIP Act contain offences for the corrupt disclosure and use of personal and health information by public sector officials and for inappropriately offering to supply personal or health information that has been disclosed unlawfully. Section 111 of the ICAC Act also makes it a criminal offence for an ICAC officer to, directly or indirectly, make a record of or release information other than for the purposes of the ICAC Act, or in accordance with the person's functions under the ICAC Act.

The ICAC minimises the risk of its officers committing any of these offences by undertaking appropriate vetting to ensure that it only employs people of the highest integrity, ensuring that officers both during their induction and continuing service with the ICAC are informed about, and provided with, training on relevant legislative provisions and ethical conduct. The ICAC also provides secure storage of, and limited access to, personal information records and regularly reviews this plan and its policies and procedures in relation to the collection, storage, retention and access to personal information.

## Devising policies and practices

The ICAC develops policies and practices by:

- examining changes in the legislative, policy or operational environment for their impact on the ICAC and its operations
- conducting regular reviews of its policies and procedures
- considering the privacy implications of changes to policies and systems to identify any procedural changes required.

The ICAC's Executive Management Group (EMG) and Senior Leadership Forum (SLF) are responsible for approving ICAC policies and procedures.

The EMG comprises the Chief Commissioner, the two Commissioners, the Chief Executive Officer and the Executive Directors of the Corporate Services, Legal, Investigation and Corruption Prevention divisions. It generally meets on a quarterly basis.

The SLF comprises the Chief Executive Officer and the Executive Directors of the Corporate Services, Legal, Investigation and Corruption Prevention divisions. It generally meets on a fortnightly basis.

Generally, new policies and procedures and significant changes to existing policies and procedures are considered and approved by the EMG. Less significant changes to policies and procedures are considered and approved by the SLF.

There are various ICAC policies that affect the handling of personal information by the ICAC.

The ICAC Code of Conduct (ICAC Policy 9) sets out the general standards of conduct expected of ICAC officers, including the use and protection of personal information.

The Personal Information Policy (ICAC Policy 47) outlines arrangements concerning the protection of confidential information held by the ICAC's People, Governance and Security Section. This policy provides further information on what records are collected by the ICAC, the purpose of their collection, their storage, and also who has access to relevant records and the purposes for which access may be granted.

The Records Management Program Policy and Procedure (ICAC Policy 66) sets out arrangements for the capture, creation, control and maintenance of electronic and physical records.

The Information Technology Security Policy (ICAC Policy 78) ensures that information managed by the ICAC is appropriately secured and that a process of risk assessment is carried out to determine the appropriate security levels.

The Information Management and Technology (IM&T) Acceptable Usage Policy (ICAC Policy 108) ensures that ICAC officers are aware of their obligations when using IM&T resources, outlines the conditions for use of IM&T resources and supports the requirements of the NSW Government Cyber Security Policy.

### Dissemination of policies and practices

All ICAC officers are required to familiarise themselves and comply with ICAC policies and procedures.

All external contractors and consultants are notified of applicable ICAC policies.

All ICAC policies and procedures are published on the ICAC intranet, which is accessible to all ICAC officers. Members of the public may access the ICAC Code of Conduct by visiting the ICAC's website at www.icac.nsw.gov.au.

All ICAC officers are notified via internal email of any amendments or changes to existing policies or procedures and all new policies and procedures.

This PMP is available on the ICAC intranet and internet sites.

## 5. How to access and amend personal and health information

ICAC officers and others seeking to access or amend any of their personal information (including health information) held by the ICAC in relation to its administrative or educative functions may contact the ICAC Executive Director of Corporate Services at icac@icac.nsw.gov.au.

The PPIP Act and HRIP Act do not generally give people the right to access someone else's personal information.

Section 26 of the PPIP Act provides that a person can give consent for their personal information to be disclosed to someone who would not otherwise be entitled to access to that information.

Sections 7 and 8 of the HRIP Act provide that an authorised person can act on behalf of someone else. The health privacy principles also contain information about other reasons the ICAC may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual, to find a missing person or for compassionate reasons.

There is no fee to access or amend personal information.

## Informal request

A person wishing to access or amend their personal information in relation to the Commission's administrative and educative functions does not need to make a formal written request, although, depending on the circumstances, the ICAC may request a written application. An informal request may be made to the ICAC officer handling the matter or the Executive Director, Corporate Services at icac@icac.nsw.gov.au.

A person may also make an informal complaint if they consider the ICAC has breached the PPIP Act or HRIP Act in relation to their personal information.

The ICAC will respond to informal requests and complaints within five working days. If it is not possible to finalise the matter within that time, the ICAC will advise the person how long it will take and will subsequently contact the person to advise the outcome of the request.

If a person is dissatisfied with the outcome of an informal request, then they may make a formal application (see below).

## Formal application

A person may make a formal written application to access or amend their personal information in relation to the ICAC's administrative and educative functions without first making an informal request.

A formal application should be made to the ICAC's Privacy Contact Officer (see contact details below). The application should:

- include the person's name and, if the person is not an ICAC officer, their contact details
- state whether the person is making the application under the PPIP Act (personal information) or the HRIP Act (health information)
- explain what personal or health information the person wishes to access or amend
- explain how the person wants to access or amend the information.

The ICAC aims to provide a written response within 10 working days. If it is not possible to finalise the matter within that time, the ICAC will advise the person how long it will take and will subsequently contact the person to advise the outcome of the application.

If a person thinks it is taking an unreasonable amount of time to respond to an application, they have the right to seek an internal review.

In addition, a person may make an application under the *Government Information (Public Access) Act 2009* for access to government information. Such an application should be sent to the Solicitor to the Commission at icac@icac.nsw.gov.au. Any such application will be determined on the basis set out in that Act.

### What happens if an application is refused?

If the ICAC decides not to give access to or amend personal or health information, it will explain the reasons.

If the person disagrees with the decision, they can seek an internal review.

## 6. Procedures for review

### Internal review

If a person considers that the ICAC has breached an information protection principle or a health privacy principle (in relation to the exercise of the ICAC's administrative and educative functions) or has otherwise breached the PPIP Act or HRIP Act relating to their personal or health information, then the person is entitled to seek an internal review.

Some individuals with privacy concerns may not want to go through a formal internal review process. In cases where individuals have a minor privacy concern that can be resolved quickly, they may raise their concern with the Solicitor to the Commission at icac@icac.nsw.gov.au. Any such complaint will be dealt with as expeditiously as possible.

Applications for review should be made within six months of the person becoming aware of the conduct complained about. Applications made after this time may be declined.

Applications for formal review must be in writing, contain the applicant's contact details and be addressed to the Solicitor to the Commission.

Internal reviews will be conducted by the Solicitor to the Commission, unless the Solicitor to the Commission is substantially involved in any matters relating to the conduct the subject of the application, in which case the Chief Executive Officer will appoint another officer to conduct the review.

In conducting an internal review, the reviewer will comply with Part 5 of the PPIP Act.

On receipt of any application for review, the reviewer will notify the Privacy Commissioner of the application (in accordance with s 54 of the PPIP Act) and keep the Privacy Commissioner informed of the progress and outcome of the internal review.

The reviewer will acknowledge receipt of an internal review application within five working days.

Any review will be completed as soon as reasonably practicable. If the review is not completed within 60 days from the date of its receipt by the ICAC, the applicant is entitled to make an application under s 55 of the PPIP Act to the NSW Civil and Administrative Tribunal (NCAT) for a review of the relevant conduct.

After completing the review, the ICAC may do any one or more of the following:

- take no further action on the matter
- make a formal apology to the applicant
- take such remedial action as it thinks appropriate
- provide undertakings that the conduct will not occur again
- implement administrative measures to ensure the conduct will not occur again.

As soon as practicable (or in any event within 14 days) after the completion of any review by the ICAC, it will notify the applicant in writing of the outcome of the review, the actions proposed to be taken by the ICAC (and the reasons for taking that action) and the right of the person to have those findings and the proposed action reviewed by NCAT.

## External review

A person must seek an internal review before they have a right to seek an external review.

Section 55 of the PPIP Act provides that a person may seek an external review under the *Administrative Decisions Review Act 1997* if the person is dissatisfied with the finding of the internal review or the action taken by the ICAC in relation to the application.

To seek an external review, a person must apply to NCAT, which has the power to make binding decisions on an external review.

Information about seeking an external review, including what forms to use and what fees are payable, can be obtained from the NCAT website at: www.ncat.nsw.gov.au, by visiting NCAT at Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney or phoning 1300 006 228.

An order or other decision made by NCAT may be appealed.

## Public interest disclosures

A person may make a public interest disclosure under the *Public Interest Disclosures Act 2022* (“the PID Act”) in relation to “serious wrongdoing”, including a privacy contravention.

A privacy contravention means a failure, other than a trivial failure, by an agency or public official to exercise functions in accordance with the PPIP Act or HRIP Act.

A public interest disclosure should be made in accordance with the PID Act.

A public interest disclosure about personal information privacy contraventions may be made to the Privacy Commissioner.

The ICAC's public interest disclosure policies for external reports and officers of the Commission are available on the ICAC's website.

## 7. Privacy Commissioner complaints

Section 45 of the PPIP Act provides that a complaint may be made to the Privacy Commissioner about an alleged violation of, or interference with, the privacy of an individual.

A complaint may be in writing or verbal, but the Privacy Commissioner may require a complaint to be put in writing.

A complaint must be made in writing within six months (or such later time as the Privacy Commissioner may allow) from the time the complainant first became aware of the conduct or matter the subject of the complaint.

The Privacy Commissioner may be contacted by:

Email: ipcinfo@ipc.nsw.gov.au
Telephone: 1800 472 679
Post: GPO Box 7011, Sydney NSW 2001
Office attendance via pre-arranged appointment:
Level 15, McKell Building, 2–24 Rawson Place, Haymarket NSW 2000.

## 8. Data breach policy

Amendments to the PPIP Act (Part 6A), which came into effect on 28 November 2023, impact the responsibilities of the ICAC under the PPIP Act by introducing a Mandatory Notification of Data Breach Scheme ("the MNDB Scheme"), requiring it to provide certain notifications in the event of an "eligible data breach" of personal or health information.

An "eligible data breach" means:

a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or
b) personal information held by a public sector agency is lost in circumstances where –
    i. unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

ii. if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would likely result in serious harm to an individual to whom the information relates.

The MNDB Scheme requires public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm.

The MNDB Scheme requires agencies to satisfy other data management requirements, including to maintain an internal data breach incident register for eligible data breaches and have a publicly-accessible data breach policy.

Under the MNDB Scheme, agencies have an obligation to:

- immediately make all reasonable efforts to contain a data breach
- undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach
- during the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach
- decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is an eligible data breach
- notify the Privacy Commissioner of the eligible data breach
- notify individuals affected by the eligible data breach or publish notification on the public notification register (unless exempted from doing so under sections 59S, 59T, 59U, 59V, 59W or 59X of the PPIP Act)
- comply with other data management requirements.

The ICAC has a Data Breach Policy that sets out its procedures for managing a data breach, including the assessment and notification requirements for the MNDB Scheme. The Data Breach Policy can be accessed **here**.

## 9. Promoting this PMP

The ICAC is committed to compliance with the PPIP Act and HRIP Act. It reinforces transparency and compliance by:

- writing the PMP in plain English
- endorsing the PMP
- making it available to ICAC officers on the staff intranet and publicly available on the ICAC website
- ensuring the PMP is regularly reviewed and updated or amended as appropriate
- reporting on privacy issues in the ICAC's annual report in accordance with the provisions of the ICAC Act and *Government Sector Finance Act 2018*
- identifying privacy issues when implementing new systems
- ensuring appropriate and up-to-date policies and procedures are in place relating to the collection, retention and security of personal information, ensuring these are communicated to and understood by staff, and ensuring they are enforced.

# 10. Contacting the ICAC

## ICAC Privacy Contact Officer

The Solicitor to the Commission is the ICAC's Privacy Contact Officer.
The Privacy Contact Officer:

- responds to enquiries about how the ICAC manages personal and health information
- provides guidance on broad privacy issues and compliance
- where appropriate, conducts internal reviews about possible breaches of the PPIP Act and HRIP Act (unless the subject of the review is the conduct of the Privacy Contact Officer).

## The ICAC's contact details

| | |
|---|---|
| Postal Address: | The Solicitor to the Commission<br>NSW ICAC<br>GPO Box 500<br>SYDNEY NSW 2001 |
| Telephone: | (02) 8281 5999 |
| Street Address: | Level 7, 255 Elizabeth Street<br>Sydney, NSW 2000 |
| Email: | icac@icac.nsw.gov.au |

# 11. Other matters

Apart from the PPIP Act and the HRIP Act, other legislation also affects the way in which the ICAC and its officers deal with "personal information", including personal information obtained by the ICAC during the course of its investigative and complaint-handling functions.

Of particular importance is s 111 of the ICAC Act, which applies to current and former ICAC officers. That section makes it an offence for a person to directly or indirectly, except for the purposes of the ICAC Act or otherwise in connection with the exercise of the person's functions under the ICAC Act, make a record of any information or divulge or communicate to any person any information, being information acquired by the person by reason of, or in the course of, the exercise of the person's functions under the ICAC Act.

Other legislation, set out in Appendix A, is also relevant to the treatment of personal information.

# APPENDIX A

## Legislation affecting process of information

### *Crimes Act 1900*

Part 6 of this Act creates offences for unauthorised obtaining of access to or interference with data in computers. There are higher penalties for accessing certain categories of sensitive government information such as law enforcement information or for alteration or destruction of data.

### *Criminal Records Act 1991*

Restricts access to, and disclosure of, spent and quashed convictions.

### *Government Information (Public Access) Act 2009* and *Government Information (Public Access) Regulation 2018*

Deals with applications for access to government information that may contain personal information. If an application concerns another person's personal or health information, the ICAC must consult with the affected party and must not disclose the information until the affected party has had an opportunity to seek review of any decision to grant access to the information.

This Act does not apply to the ICAC in relation to the ICAC's corruption prevention, complaint handling, investigative and report functions.

### *State Records Act 1998* and *State Records Regulation 2015*

Defines the circumstances under which public sector agencies can dispose of their records and authorises the State Records Authority to establish policies, standards and codes to ensure adequate records management by public sector agencies.