INDEPENDENT COMMISSION AGAINST CORRUPTION

PRIVACY MANAGEMENT PLAN

OCTOBER 2018

INTRODUCTION

This plan sets out how the Independent Commission Against Corruption (the ICAC) manages personal and health information.

This plan was approved on 31 October 2018 and replaces the ICAC's previous plan adopted in 2013.

Why the ICAC has a plan

Section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires each public sector agency to have a privacy management plan.

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

What this plan covers

Section 33(2) of the PPIP Act requires that a privacy management plan must include provisions relating to the following:

(a) the devising of policies and practices to ensure compliance by the agency 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 agency,

(c) the procedures that the agency proposes to provide in relation to internal review under Part 5 of the PPIP Act,

(d) such other matters as are considered relevant by the agency in relation to privacy and the protection of personal information held by the agency.

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.

ABOUT THE ICAC

The ICAC is a statutory corporation established by the *Independent Commission Against Corruption Act 1988* (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.

The ICAC's aims are to protect the public interest, prevent breaches of public trust and guide the conduct of public officials.

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

Application of information protection and health privacy principles

The PPIP Act sets out 12 information protection principles. 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 the exercise by the ICAC of its administrative and educative functions.

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.

HOW THE ICAC MANAGES PERSONAL AND HEALTH INFORMATION

The ICAC collects and receives different kinds of information in order to conduct its functions. In this section, a reference to personal information includes a reference to health information.

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 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. 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.

3. Workers' compensation records containing information relating to an injury or illness and other medical information provided by staff.

4. Information relating to vetting of prospective employees, consultants and contractors including information relating to associates.

5. 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.

6. Images captured by the ICAC's close 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.

7. 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. Our systems comply with the international standard of information security ISO 27001.

Access to particular personal information is restricted to those key ICAC officers deemed to require access to that information in order to perform their functions and to the person to whom the information relates. Hard copy material is mainly located at the ICAC's office at 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 access. 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 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 a person 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 employees committing any of these offences by undertaking appropriate vetting to ensure that it only employs staff of the highest integrity, ensuring that staff both during their induction and continuing service with the ICAC are informed about and provided with training on relevant legislative provisions and ethical conduct, providing secure storage of and limited access to personal information records and regularly reviewing 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's Executive Management Group (EMG) is responsible for approving all ICAC policies and procedures. The EMG comprises the Chief Commissioner, the two Commissioners, the Chief Executive Officer and Executive Directors of the Corporate Services, Legal, Investigation and Corruption Prevention divisions.

There are various 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 Human Resources & Administration 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 External Systems Access Policy (ICAC Policy 63) sets out principles for access to and use of information obtained from external systems.

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.

Dissemination of policies and practices

All ICAC officers are required to familiarise themselves with 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 site, which is accessible to all ICAC officers. Members of the public may access the ICAC Code of Conduct by going to the ICAC's website at: www.icac.nsw.gov.au. Members of the public may request access to the other policies specified above by writing to the Solicitor to the Commission.

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

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

HOW TO ACCESS AND AMEND PERSONAL AND HEALTH INFORMATION

ICAC officers and others seeking to amend their personal information (including health information) held by the ICAC in relation to its administrative or educative functions may request amendments by contacting the ICAC Executive Director of Corporate Services.

Informal request

A person wishing to access or amend his or her personal information 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.

The ICAC will respond to informal requests 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 unhappy with the outcome of an informal request then the person may make a formal application.

Formal application

A person may make a formal written application to access or amend his or her personal information 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, the person's 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 ten 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. Any such application will be determined on the basis set out in that Act.

Why an application may be 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 outcome of an application, they can seek an internal review.

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.

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. 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 Commissioner 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:

a) take no further action on the matter,

b) make a formal apology to the applicant,

c) take such remedial action as it thinks appropriate,

d) provide undertakings that the conduct will not occur again,

e) 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, the ICAC 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 the person has a right to seek an external review.

A person may seek an external review if the person is unhappy with the finding of the internal review or the action taken by ICAC in relation to the application.

To seek an external review, a person must apply to NCAT.

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, or by visiting NCAT at Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney or phoning 1300 006 228.

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

PROMOTING THE PLAN

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

- endorsing the privacy management plan and making it publicly available on the ICAC website,
- ensuring the plan 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 *Annual Reports (Departments) Act 1985*,
- 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 are enforced.

CONTACTING THE 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, and
- 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 ICAC GPO Box 500 SYDNEY NSW 2001
Phone:	(02) 8281 5999
Street Address:	Level 7, 255 Elizabeth Street Sydney, NSW 2000
Email:	icac@icac.nsw.gov.au

OTHER MATTERS

Apart from the PPIP Act and the HRIP Act other legislation also affects the way in which the ICAC and ICAC 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. It 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 PROCESSING 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 1988 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.