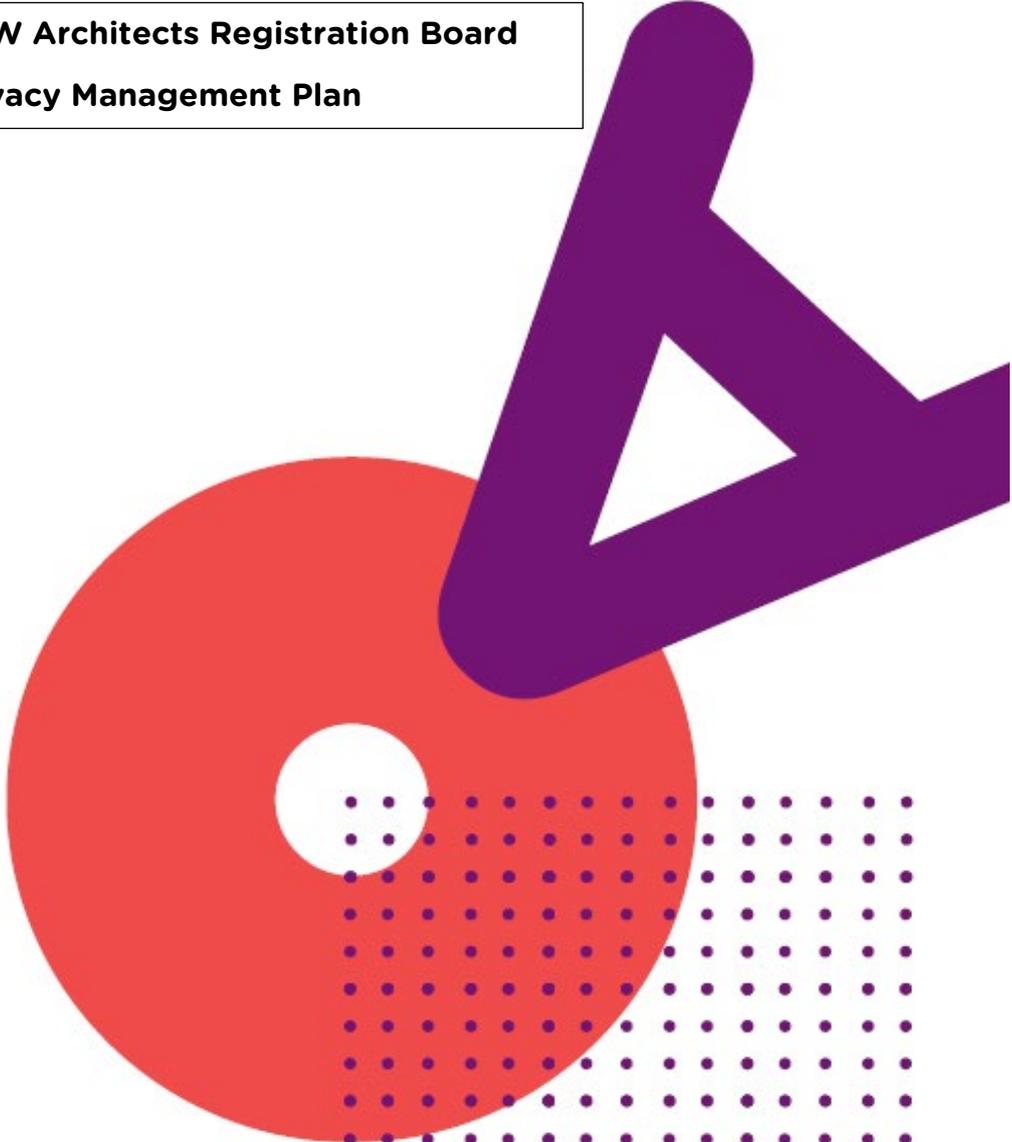


**NSW Architects Registration Board  
Privacy Management Plan**



NSW  
Architects  
Registration  
Board



## Contents

Objective of a privacy management plan .....	3
Definitions .....	3
Board functions and the types of personal and health information we hold .....	4
Responsibilities of all employees and Board Members .....	4
Managing Personal and Health Information .....	5
1. Collection of personal information must only be for a lawful purpose (IPP 1 [PPIP s8] and HPP 1) .....	5
2. Personal information must only be collected directly from the person the information is about or someone authorised by that person (IPP 2 [PPIP s9] and HPP 3) .....	5
3. Notification when collecting personal information (IPP 3 [PPIP s10] and HPP 4) .....	6
4. How we collect personal information - the method and content (IPP 4 [PPIP s11] and HPP 2) .....	6
5. How we store and secure personal and health information (IPP 5 [PPIP s12] & HPP 5) .....	7
6. Transparency (IPP 6 [PPIP s13] and HPP 6) .....	7
7. Access to information we hold (IPP 7 [PPIP s14] and HPP 7) .....	8
8. Correction of information we hold (IPP 8 [PPIP s15] and HPP 8) .....	8
9. Accuracy of information (IPP 9 [PPIP s16] and HPP 9) .....	9
10. How we use personal and health information (IPP 10 [PPIP s17] and HPP 10) .....	9
11. How we disclose personal and health information (IPP 11 [PPIP s18] and HPP 11) .....	9
12. Stricter rules apply to specific information (IPP 12 [PPIP s19] and HPP 14) .....	10
13. How we use unique identifiers and linkage of health records (HPP 12, 13 and 15) .....	10
Exemptions - Sometimes Information Protection and Health Privacy Principles do not apply .....	11
Information published on public registers (Part 6 of the PPIP Act) .....	11
Internal Reviews and Complaints .....	11
External Review by NCAT .....	12
Offences under the PPIP Act and HRIP Act .....	12
Raising Awareness of/using the plan .....	13
Contacts .....	14

## Objective of a privacy management plan

The NSW Architects Registration Board's (the 'Board') Privacy Management Plan (PMP) explains how we manage personal and health information in line with NSW privacy laws.

The Board is required to have a PMP under the privacy laws. We collect and handle the personal or health information of many people across the NSW architecture profession. The Board takes seriously its responsibility to look after the personal and health information it collects and handles relating to consumers, registered architects, candidates for the Architectural Practice Examination (APE) and NSW Portfolio Program of Assessment, employees and Board Members. The Board is bound by law in the way it notifies collection of, usage, storage and disclosure of personal and health information. To help guide the Board in how to do this, section 33 of the *Privacy and Personal Information Protection Act 1998 (PPIP Act)* requires that we have this PMP available.

Each NSW public sector agency must have a PMP and provide a copy to the NSW Privacy Commissioner. It should also be made publicly available on the agency's website and be made available in other ways on request.

In the Board's PMP you will find information about:

- how to contact the Board with an enquiry or complaint about your personal or health information;
- what to do if you think the Board has breached the *PPIP Act* or the *Health Records and Information Protection Act 2002 (HRIP Act)*;
- how to access and amend any personal and health information the Board holds about you.

Internally, the Board uses its PMP to train staff in handling personal and health information. The Board devises its policies and practices to comply with the *PPIP Act* and the *HRIP Act*.

## Definitions

The following terms are used in this PMP:

**agency** – a 'public sector agency', as defined in section 3 of the *PPIP Act*.

**personal information** – as defined in section 4 of the *PPIP Act*, personal information is information or an opinion that identifies a person (or that would allow a person's identity to be discovered). Personal information can include:

- person's name, date of birth, address, financial information, other details;
- photographs, images, video or audio footage.

Some types of personal information are exempt from the definition of personal information. This includes information concerning

- a person who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or opinion about a person's suitability for employment as a public sector official.
- health information – as defined in section 6 of the *HRIP Act*, health information is a specific type of 'personal information'. It includes but is not limited to:
  - information or an opinion about a person's physical or mental health, or a disability (at any time), such as a psychological report, blood test or x-ray;
  - personal information a person provides to a health service provider;
  - information or an opinion about a health service already provided to a person e.g. attendance at a medical appointment;
  - information or an opinion about a health service that is going to be provided to a person;
  - a health service a person has requested;
  - some genetic information.

## **Board functions and the types of personal and health information we hold**

The Board collects and holds personal or health information to carry out its daily operations. This may include information required to process initial applications for registration as an architect, applications for renewal of registration, consumer complaints about architects, staff records or requests under right to information laws. The information collected for any Board function may be used by the Board for a primary or directly-related secondary purpose as allowed under legislation. A primary purpose is the clear purpose for which we collect the information from you, for example for a registration application. Directly related secondary purposes might include investigations, policy and programs, or responding to ministerial enquiries. Your personal and health information is always handled in accordance with the privacy laws and principles.

There are two main categories of personal and health information that we hold or have access to:

- personal and health information about members of the public and stakeholders;
- personal and health information about Board Members and staff (employees and contractors).

### **Personal and health information held about members of the public and stakeholders**

To exercise the Board's various functions and activities, we hold personal or health information obtained through applications for registration as an architect and consumer complaints about architects. The following personal and health information may be collected, depending on the specific needs of the Board:

- Name, date of birth, home address and other contact details;
- Financial information such as bank details, signatures;
- Complaints and correspondence associated with their investigation;
- Employment details, job specifications and status;
- Insurance claims history;
- Medical certificates and injuries;
- Criminal records, compliance history, bankruptcy information.

### **Personal and health information held about employees**

Day-to-day operations of most employees, such as leave requests and payroll and contractual arrangements are protected and securely stored.

## **Responsibilities of all employees and Board Members**

All employees, Board Members and contractors are required to comply with the privacy principles set out in the *PPIP Act* and *HRIP Act*. Both Acts contain criminal offence provisions applicable to employees, agents and contractors who use or disclose personal information or health information other than in accordance with their lawful functions. Employees who are suspected of conduct that would breach the privacy principles or the criminal provisions may be disciplined for a breach of the Code of Conduct. Suspected criminal conduct may result in dismissal of employment and/or referral to the NSW Police.

It is an offence to:

- intentionally disclose or use personal or health information accessed in doing our jobs for an unauthorised purpose;
- offer to supply personal or health information for an unauthorised purpose;
- attempt by threat, intimidation, etc, to dissuade a person from making or pursuing a request for health information, a complaint to the NSW Privacy Commissioner about health information, or an internal review under the *HRIP Act*; or
- hinder the NSW Privacy Commissioner or an employee from doing their job.

## Managing Personal and Health Information

The *PIIP Act* and *HRIP Act* outline principles for managing personal and health information and regulate the collection, storage, usage and disclosure of personal and health information. There are 12 Information Protection Principles (IPPs) set out in Part 2, Division 1 of the *PIIP Act* and 15 Health Privacy Principles (HPPs) set out in Schedule 1 of the *HRIP Act*.

### 1. Collection of personal information must only be for a lawful purpose (IPP 1 [PIIP s8] and HPP 1)

#### 1.1. The principle in brief

The Board will only collect personal and health information if:

- it is for a lawful purpose that is directly related to one of our functions; and
- it is reasonably necessary for us to have the information.

#### 1.2 How this principle is applied by the Board

The Board will not collect personal and health information unless we need it for one of our functions. The Board may also liaise with external stakeholders to fulfil our functions under legislation and staff will seek to access the personal and health information collected by those stakeholders if it is reasonably necessary for those functions. A substantial amount of personal and health information is collected from our employees for the purpose of personnel management. Such information is stored securely. Personal and health information may also be collected directly from the employee. For example, minimal health information may be collected for the purpose of making necessary adjustments to allow the employee to work.

### 2. Personal information must only be collected directly from the person the information is about or someone authorised by that person (IPP 2 [PIIP s9] and HPP 3)

#### 2.1. The principle in brief

The Board collects personal information directly from the person unless they have authorised otherwise.

#### 2.2 How this principle is applied by the Board

The Board collects your personal information directly from you, unless you have authorised us to do otherwise. However, there are circumstances when information may have been gathered from other sources, including other government agencies, where we are lawfully authorised to do this under a legislative provision or a Privacy Code of Practice. For example, complaints or disputes lodged with the Board require one party to the dispute to provide the name and contact details of the opposing architect/s so that the Board can investigate the matter. Human resources personnel may need to liaise with an injured employee's doctor. We will take what steps are necessary to ensure that collection of such information is done lawfully, such as getting consent from an employee to contact their treating doctor.

### **3. Notification when collecting personal information (IPP 3 [PPIP s10] and HPP 4)**

#### **3.1 The principle in brief**

When collecting personal information from you, we will take reasonable steps to tell you:

- who we are and how to contact us;
- what the information will be used for;
- what other organisations (if any) we intend will receive this type of information from us;
- whether the collection is authorised by law or is voluntary;
- what the consequences will be if you do not provide the information to us;
- how you can access and correct your information held by us; and
- the name and address of the agency that is collecting the information and the agency that is to hold the information.

#### **3.2 How this principle is applied by the Board**

The Board continually reviews and refines the various forms it uses to collect personal information to ensure they include clear privacy statements. Sometimes information may be collected over the phone or face to face. Staff are trained to ensure they understand the privacy principles.

### **4. How we collect personal information - the method and content (IPP 4 [PPIP s11] and HPP 2)**

#### **4.1 The principle in brief**

When we collect personal information from you we will take reasonable steps to ensure the information we collect is relevant, accurate, up-to-date and complete, and not intrusive or excessive.

#### **4.2 How this principle is applied by the Board**

We will take reasonable steps to ensure that when we design forms, communicate with members of the public, architects and employees (face-to-face, over the phone and in writing), or otherwise collect information from you, we do not seek personal information that is intrusive or excessive. We will ensure that the personal information we do collect is relevant, accurate, up-to-date and complete. We may do this by cross referencing the information with other sources, such as the Australian Securities and Investment Commission's (ASIC) register of companies and business names. We will also make sure that, if you request it, you can see what information we hold about you and we will correct it as necessary. We design forms to ensure that only information required to carry out our functions is requested or required from you. We will ensure these privacy principles are built into our policies, procedures and practices through staff training.

## **5. How we store and secure personal and health information (IPP 5 [PPIP s12] and HPP 5)**

### **5.1 The principle in brief**

We take reasonable security measures to protect personal and health information from loss, unauthorised access, modification, use or disclosure. We ensure personal and health information is stored securely, not kept longer than necessary, and disposed of appropriately.

### **5.2 How this principle is applied by the Board**

We consider the security of information to be an important issue and have systems in place to ensure that only authorised people can access information. In addition, the *PPIP Act* carries several provisions for prosecuting individuals for unlawful disclosure of personal and health information. Unlawful access to information by our employees or contractors will result in disciplinary action, and in some serious cases, in criminal prosecution.

We use technical, physical and administrative actions, as well as assessment by independent audit, as security measures to ensure personal and health information is stored securely. Some examples of retention and security measures that we have in place include:

- All our databases that hold personal or health information are restricted by password or other security measures to ensure that only people with a reason have access to that information;
- Secure destruction bins or paper shredders are provided for disposal of confidential paper records.

The Board stores information in accordance with the provisions of the *State Records Act 1998* and standards issued by State Archives NSW.

## **6. Transparency (IPP 6 [PPIP s13] and HPP 6)**

### **6.1 The principle in brief**

Once we have confirmed your identity, we will take reasonable steps to let you find out whether we are likely to hold your personal or health information, the nature of the information we hold, the purposes for which we have used your personal or health information, and how you can access your information.

### **6.2 How this principle is applied by the Board**

We have a broad obligation to the community to be open about how we handle personal and health information. The PMP for the Board is available on the website. The PMP sets out the major categories of personal and health information that is held, explains the privacy obligations, and explains the process for accessing and/or amending any of the personal and health information we hold about you.

## **7. Access to information we hold (IPP 7 [PPIP s14] and HPP 7)**

### **7.1 The principle in brief**

You can make enquiries at any time to find out the personal or health information we hold about you. Once we have confirmed your identity, you may access your personal and health information without unreasonable delay or expense. We will only refuse access where authorised by law. If requested, we will provide written reasons for any refusal in line with our commitment to be open and transparent.

### **7.2 How this principle is applied by the Board**

If you want a copy of your own personal or health information held by Board, we will usually be able to provide it to you, free of charge. If you are having difficulties accessing your personal or health information, or you wish to make a formal application for information, you can contact the Board by email to [mail@architects.nsw.gov.au](mailto:mail@architects.nsw.gov.au).

## **8. Correction of information we hold (IPP 8 [PPIP s15] and HPP 8)**

### **8.1 The principle in brief**

Once we have confirmed your identity, you may update or amend your personal or health information held by us to ensure it is accurate, relevant, up-to-date, complete, and not misleading.

### **8.2 How this principle is applied by the Board**

The Board may wish to verify the accuracy of any information you request to be amended, such as confirming qualifications with the provider or information about a bankruptcy with the Bankruptcy Trustee. In general, any proposed corrections to your personal or health information should be provided in writing so we can verify your identity and keep a record of the correction. You can send any requests for correction of your information to [mail@architects.nsw.gov.au](mailto:mail@architects.nsw.gov.au).

We must provide you access to, or amend, your personal or health information without excessive delay or expense. We do not charge any fees to access or amend your personal or health information unless you are lodging a formal application under the *Government Information (Public Access) Act 2009 (GIPA Act)*.

If the Board does not agree to the correction or amendment, the reason for the refusal will be provided in writing to person the information refers to and the applicant requesting the amendment. The request to amend, and any reason for a refusal to amend, must be saved adjacent to the information it refers to for the life of the information record.

A disputed record may be a professional opinion that is challenged; however, the record of the professional opinion must be maintained regardless of the individual's request to vary that opinion.

## **9. Accuracy of information (IPP 9 [PPIP s16] and HPP 9)**

### **9.1 The principle in brief**

Before using personal or health information we take reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

### **9.2 How this principle is applied by the Board**

We ensure the accuracy of the information by collecting it directly from you wherever practicable. This gives you the opportunity to correct the information and allows us to ensure the information is relevant, accurate, up-to-date, complete and not misleading prior to the use of the information. We take such steps as are reasonable in the circumstances to ensure the accuracy of information. This may be achieved through the requirement of supporting documentation or by confirming the information with an outside agency. At any point in time, architects can login to their personal account and update their details and the Board issues an annual reminder to provide architects with the opportunity to correct inaccuracies in their personal details.

## **10. How we use personal and health information (IPP 10 [PPIP s17] and HPP 10)**

### **10.1 The principle in brief**

We may use personal and health information for the primary purpose for which it was collected and for a directly related secondary purpose (e.g. use information from a consumer complaint in an investigation about an architect), if

- we believe the use is necessary to prevent or lessen a serious and imminent threat to life or health;
- it is lawfully authorised or required;
- required for another purpose, if you have consented.

### **10.2 How this principle is applied by the Board**

As a general principle, we use the personal and health information we've collected only for the purpose for which it was collected. The relevant purpose should have been set out at the time of collection.

## **11. How we disclose personal and health information (IPP 11 [PPIP s18] and HPP 11)**

### **11.1 The principle in brief**

We may disclose your information if you have consented and the information is not 'health information' or 'sensitive information' and you have been made aware that the information is likely to be disclosed to the recipient: if it is lawfully authorised or required; if it is reasonably necessary to lessen or prevent a serious threat to health; if the information is 'health information' and the disclosure is for the purpose for which the information was collected; or for a directly related secondary purpose within your reasonable expectations.

### **11.2 How this principle is applied by the Board**

We may disclose information we are lawfully authorised or required to disclose, such as where a public register is required to be kept by law. Other disclosures we make will be appropriately related to the purpose for which the information was collected, or we will have your consent. We also disclose personal information to other government agencies where it is lawful. When we are required to disclose information between other public sector agencies, we will do so in accordance with the privacy laws.

## **12. Stricter rules apply to specific information (IPP 12 [PPIP s19] and HPP 14)**

### **12.1 The principle in brief**

Disclosing sensitive information (e.g. your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities) is only allowed with your consent or if there is a serious and imminent threat to a person's life or health. Disclosing personal or health information to someone outside of NSW, or to a Commonwealth agency, is only permitted in limited circumstances as set out in the legislation.

### **12.2 How this principle is applied by the Board**

We make every effort to minimise the amount of information we collect about your ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities. Where this information is collected, it is treated with the highest protection wherever possible.

## **13. How we use unique identifiers and linkage of health records (HPP 12, 13 and 15)**

### **13.1 The principle in brief**

We may only assign identifiers (e.g., a number) to an individual's health information if it is reasonably necessary. We must not include health information in a health records linkage system without your consent.

### **13.2 How this principle is applied by the Board**

Health information is generally only collected by the Board to manage cases of injured employees and to investigate workplace incidents. Where health information has been gathered to case manage an injured employee, it is not given a separate identifier but kept against the relevant employee's injury management record. Where the information has been gathered as part of an investigation of a workplace incident, the information is held against the investigation file, and not given any separate identifier. The Board has no linkages to any health records systems.

The Board may inadvertently collect health information, even though it is not sought. When this sort of information is collected, it is not given any separate identifier and is not included in any health records linkage system.

## **Exemptions - Sometimes the Information Protection Principles and Health Privacy Principles do not apply**

The IPPs and HPPs do not apply in certain situations or to certain information collected. Some of the key situations where collection, usage or disclosure of information is exempted from the compliance with certain IPPs and HPPs include:

- unsolicited information, unless we have retained it for a purpose (although we will generally treat unsolicited information in the same manner as information, we have requested from you);
- personal information collected before 1 July 2000 (although we will generally treat this information in the same manner as information collected after 1 July 2000);
- health information collected before 1 September 2004 (although we will generally treat this information in the same manner as information collected after 1 September 2004);
- law enforcement and investigative purposes and some complaints handling purposes;
- when authorised or required by a subpoena, warrant or statutory notice to produce;
- if another law authorises or requires us not to comply;
- where non-compliance is otherwise permitted, implied or contemplated by another law;
- in the case of health information, to lessen or prevent a serious threat to public health or public safety;
- some research purposes;
- in the case of health information, compassionate reasons, in certain limited circumstances;
- finding a missing person information sent between public sector agencies to transfer enquiries or to manage correspondence from a Minister or member of Parliament;
- The privacy management plans of divisions will provide examples of any relevant laws or circumstances that require or permit non-compliance with the IPPs or HPPs.

## **Information published on public registers (Part 6 of the PPIP Act)**

A public register is a register of information that is publicly available or open to public inspection. If you hold an authority that is required to be published on a public register such as a registration as an architect in NSW, some of your personal information will be publicly available, such as your name, address, and any conditions placed on the registration.

If you have any specific concerns about your personal information being on a public register, you can contact [mail@architects.nsw.gov.au](mailto:mail@architects.nsw.gov.au). Any request for your information to be suppressed from a public register must be in writing and must provide reasons for the request, and include other supporting documents if relevant. In making any decision to suppress your information, we will balance your rights with the public interest in maintaining public access to the information, in accordance with legal requirements.

## **Internal Reviews and Complaints**

If you have any concerns about the way your personal or health information has been handled, or you disagree with the outcome of your request to access or amend your personal or health information, you have the right to both an internal review of the decision by the Board or external review by the Information Privacy Commission NSW (IPC) or NSW Civil and Administrative Tribunal (NCAT), depending on the situation.

An informal request means that you contact the Board and ask for the information you are seeking. There are no fees required and no formal requirements to be met before your request will be actioned.

### What you can expect from the Board from a formal request

- Your application will be acknowledged in writing and the acknowledgement will include an expected completion date;
- The review will be conducted by a privacy officer who is an employee or an officer of the Board, qualified to deal with the subject matter of the complaint and not the subject of the complaint;
- The internal review will be completed within 60 days of receiving your application. If the review is not completed within this time, you have the right to seek an external review at NCAT;
- We will follow the NSW Privacy Commissioner's [Internal Review Checklist available here](#) and will give consideration to any relevant material submitted by you and/or the NSW Privacy Commissioner;
- In making a decision, we may decide to take appropriate remedial action, make a formal apology to you, implement administrative measures to ensure that the conduct will not occur again, undertake to you that the conduct will not occur again, and/or take no further action on the matter;
- You will be informed of the outcome within 14 days of the internal review being completed, including the findings of the review, the reasons for those findings, the action the Board proposes to take, the reasons for the proposed action (or no action), and your entitlement to have the findings and the reasons for the findings reviewed by NCAT.

### Role of the NSW Privacy Commissioner

The *PIIP Act* requires that the NSW Privacy Commissioner be informed of the receipt of an application for an internal review of conduct and receive regular progress reports of the investigation. In addition, the Commissioner is entitled to make submissions about the application for internal review. When we receive your application, we will provide a copy to the Privacy Commissioner. We will then continue to keep the Privacy Commissioner informed of the progress of the internal review, the findings of the review and the proposed action to be taken by us in response to the internal review. Any submissions made by the Privacy Commissioner to us will be taken into consideration when making our decision.

### External Review by NCAT

If you are unhappy with the outcome of the internal review, you can apply to NCAT to review the decision (an "external review"). You may also apply to NCAT to conduct an external review if we have not completed your internal review within 60 days. Generally, you have 28 days from the date of our internal review decision to seek an external review. NCAT has the power to make binding decisions on an external review, including ordering the payment of damages of up to \$40,000.

### Offences under the *PIIP Act* and *HRIP Act*

An employee or a person must not induce or attempt to induce a public sector official by way of a bribe or other corrupt conduct to disclose any personal information about another person to which the official has or had access in the exercise of his or her official functions. Maximum penalty is 100 penalty units or imprisonment for 2 years or both.

A disclosure by the NSW Privacy Commissioner or an employee without consent of the person the subject of the information attracts a penalty of 10 penalty units. A person must not make false statements or mislead the NSW Privacy Commissioner in the exercise of functions under the Act, with a penalty of 10 penalty units.

## Raising Awareness of / using the plan

Our plan will be reviewed at a minimum every two years (i.e. next review in March 2023), but more frequently when legislative, administrative, or systemic changes occur that affect the way we manage the personal and health information we hold.

The Board aims to educate members of the public about its privacy obligations by publishing its PMP on the website and by mentioning it on forms that collect personal or health information.

### Board Members

All Board Members are committed to transparency about how we comply with the *PPIP Act* and *HRIP Act*, which is reinforced by:

- endorsing the plan and making it publicly available;
- reporting on privacy in our annual report in line with the *Annual Reports (Departments) Act 1985* and *Annual Reports (Departments) Regulation 2015*; and
- using the PMP as part of the Board induction for new employees, Board Members and contractors.

### Employees

We make sure our employees are aware of this plan and how it applies to the work they do by:

- training staff so they understand their privacy obligations and how they are to manage personal and health information;
- providing targeted training for employees who work in areas with a higher exposure to the personal and/or health information of customers or staff, such as those who perform human resources functions, process applications and claims, handle frontline counter and phone enquiries, and assist with dispute resolution;
- providing refresher training so that staff maintain awareness of privacy in doing their daily business;
- writing this plan in a practical way so staff can understand what their privacy obligations are, how to manage personal and health information in their work and what to do if unsure about their privacy obligations; and
- highlighting the plan at least once a year .

## Contacts

For further information about this plan, the personal and health information held by the Board, or if you have any questions or concerns, please use the following contact details:

### **NSW Architects Registration Board**

Phone: 02 9241 4033  
Email: [mail@architects.nsw.gov.au](mailto:mail@architects.nsw.gov.au)  
Web: [www.architects.nsw.gov.au](http://www.architects.nsw.gov.au)  
Mail: Level 2, 156 Gloucester Street, The Rocks NSW 2000

### **Department of Customer Service**

Phone: 02 9372 7088  
Email: [privacy@customerservice.nsw.gov.au](mailto:privacy@customerservice.nsw.gov.au)  
Web: [www.customerservice.nsw.gov.au](http://www.customerservice.nsw.gov.au)  
Mail: Level 22, McKell Building, 2-24 Rawson Pl, Sydney NSW 2000  
Visit: Documents, enquiries or complaints can be lodged via any Service NSW centre. The Service NSW centre locator can be found at <https://www.service.nsw.gov.au/service-centre> or phone 13 77 88

### **The Information and Privacy Commission (IPC)**

Phone: 1800 472 679  
Email: [ipcinfo@ipc.nsw.gov.au](mailto:ipcinfo@ipc.nsw.gov.au)  
Web: [www.ipc.nsw.gov.au](http://www.ipc.nsw.gov.au)  
Mail: GPO Box 7011 Sydney NSW 2001  
Office: Level 15 McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

### **The NSW Civil and Administrative Tribunal (NCAT)**

Phone: 1300 006 228 and select Option 3 for all Administrative and Equal Opportunity and Occupational Divisions enquiries  
Web: [www.ncat.nsw.gov.au](http://www.ncat.nsw.gov.au)  
Post: NSW Civil & Administrative Tribunal, Administrative and Equal Opportunity Division and Occupational Division, PO Box K1026, Haymarket NSW 1240