

City of Sydney Privacy Management Plan

City of Sydney
Town Hall House
456 Kent Street
Sydney NSW 2000

Contents

Introduction	2
About the City	3
What is personal and health information	4
How the City collects and manages personal and health information	5
Public Registers	8
How to access and amend personal and health information	9
Data breaches	10
Review rights and complaints	11
Promoting privacy	13
Privacy and other legislation	14
Exemptions, directions and codes of practice	18
Contact details	19
Approval	20
Appendix A – privacy complaint: internal review application form	21

Introduction

This Privacy Management Plan (Plan) explains how the City of Sydney Council (City) manages personal and health information.

Why the City has a privacy management plan

This Plan explains how the City manages personal information in line with the *Privacy and Personal Information Protection Act 1998* (NSW) (PIIP Act) and health information in accordance with the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act). The City is required to have a Plan under s33 of the PIIP Act.

This Plan also explains how to contact the City about the personal and health information it holds, how information can be accessed and amended and how privacy complaints are handled.

What this Plan covers

Section 33(2) of the PIIP Act sets out the requirements of this Plan. This Plan must include:

- information about the City's policies and practices to ensure compliance with the PIIP Act and the HRIP Act;
- how employees, contractors and volunteers are made aware of these policies and practices;
- the internal review procedures; and
- anything else considered relevant to the Plan in relation to privacy and the personal and health information the City holds.

Any reference to employees in this document also includes reference to contractors and volunteers.

When this plan will be reviewed

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 City.

About the City

The City of Sydney Council has responsibilities under the *Local Government Act 1993* and other Commonwealth and NSW laws including the *Environmental Planning and Assessment Act 1979*, the *Public Health Act 2010*, the *Companion Animals Act 1998*, the *State Records Act 1998* and the *Government Information (Public Access) Act 2009*

Councils exist to:

- Provide a representative, informed and responsible decision-making body.
- Develop the local community and its resources in a socially just and environmentally responsible way.
- Ensure that local public services and facilities respond effectively to community needs.

More detailed information is available on the City's [website](#).

City of Sydney Functions

Under the *Local Government Act 1993*, the City's charter requires it:

- To provide for development in the local area.
- To provide for local services and facilities that benefit ratepayers, residents and visitors.
- To promote and to provide and plan for the needs of children.
- To protect health and provide for the welfare, wellbeing and interests of the local community.
- To represent and promote the interests of ratepayers and residents.
- To establish and support organisations and programs targeting the local community.
- To protect the environment and improve local amenity.
- To attract and provide infrastructure for commerce, tourism and industry.
- To engage in long-term strategic planning on behalf of the local community.

What is personal and health information

About personal information

Personal information is defined in section 4 of the PPIP Act as any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained.

What is not personal information

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

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

About health information

Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act. Health information can include information about a person's physical or mental health such as a psychological report, blood test or an x-ray, results from drug and alcohol tests, and information about a person's medical appointments. It can also include some personal information that is collected to provide a health service, such as a name and telephone number.

How the City collects and manages personal and health information

How the City collects personal information

The City collects personal information to enable it to conduct its functions. The City assesses the level of personal information that is appropriate to be collected on a case-by-case basis. In this section, a reference to personal information is also a reference to health information.

Personal information may be collected from:

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

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

The City has a range of functions requiring or involving the collection of personal information, including:

- levying and collecting rates;
- providing services, for example, child care, libraries and waste collection;
- consultation with the community, businesses and other stakeholders;
- assessing development and major project applications;
- recording, investigating, and managing complaints and allegations;
- site inspections and audits;
- incident management;
- enforcing regulations and legislation;
- issuing approvals, consents, licences and permits;
- providing funding grants;
- maintaining the non-residential register of electoral information;
- employment; and
- fitness for work

Personal information may be collected by the City in any of the following ways:

- incident reports;
- medical assessment reports;
- submissions;
- application forms;
- CCTV footage;
- public registers;
- financial transaction records;

- contracts;
- over the phone enquiries;
- counter enquiries; and
- online services

Personal information may be collected electronically, in writing, over the telephone and in person.

Personal information provided to the City

Individuals may provide the City with personal information when they make application for employment, make enquiries and when the City delivers services to them. This can include names, contact details, opinions, health conditions, family relationships, housing or tenancy information, work and education details. Individuals may also provide the City with personal information about other people.

Privacy Protection Notice

Under section 10 of the *Privacy and Personal Information Protection Act 1998* (PPIPA), when the City collects personal information from an individual, such as their name, address, telephone number or email address, the City must make the individual aware of:

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

To ensure the City complies with the PPIPA a **Privacy Protection Notice** will be included on all forms, letters and documents that collect personal information from individuals. The City's Privacy Protection Notice appears below:

PRIVACY PROTECTION NOTICE

Purpose of collection: *the purposes for which the information is being collected*

Intended recipients: *to whom (including business units or organisations) the information will be disclosed*

Supply: *whether the supply of the information is required by law or is voluntary and any consequences for the individual if the information (or any part of it) is not provided*

Access/ Correction: *how the individual can access and correct the information*

Storage: *the name and address of the business unit that is collecting the information and the business unit that is storing the information*

The Privacy Protection Notice is included on all standard City forms and is completed and included on any document requesting personal information from individuals.

Storage, access and accuracy of personal information

Personal information is stored electronically and in physical files.

The following applies to information the City holds:

- only City employees can access personal information;
- employees will make every effort to ensure personal information is accurate before using it;
- employees will use personal information only for the purpose for which it was collected; and
- employees will not disclose personal information about a person to anyone without the consent of the person, or if legally required or permitted to disclose information.

Please refer to page 18 for details of exemptions, directions and code of practice that may affect the above.

Electronic information is stored on secure information systems. Networks will be secure and require individual logins. New systems are assessed for compliance with the PPIP Act and HRIP Act. When not being used, hard copy files and sensitive information are securely stored.

Use and disclosure of personal information

Employees use the personal information collected to:

- deliver services;
- conduct research;
- provide advice; and
- continually improve services.

Public registers

The PPIP Act governs how the City should manage personal information contained in public registers. Under the PPIP Act a public register is a register of personal information that is required by law to be made, or is made, publicly available or open to public inspection. Enquiries about public registers can be made via the City's [website](#).

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

The City's public registers include:

- Land register
- Contracts over \$150,000 awarded by the City
- Register of investments
- Register of disclosures of interest
- Register of development consents
- Register of planning agreements
- Contributions register
- Record of building certificates
- Public record of licences
- Record of impounding.

Suppression of personal information

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

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

How to access and amend personal and health information

The PPIP Act and the HRIP Act give people the right to access and amend their own information.

Members of the public wishing to access or amend personal and health information the City holds about them should contact the City's [Customer Service Centre](#). The City does not charge a fee to access and amend personal and health information.

Limits on accessing or amending information

The City is prohibited from providing one person access to another person's personal and health information. However:

- under section 26 of the PPIP Act, a person can give the City consent to disclose their personal information to someone that would not normally have access to it;
- under sections 7 and 8 of the HRIP Act, an "authorised person" can act on behalf of someone else; and
- the City 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.

Data Breaches

What is a data breach?

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to the City's data. Examples include malware, hacking and data theft, accidental loss of a paper record, laptop, or USB stick, and emails sent to the wrong recipients if they contained classified material or personal information.

How does the City manage a data breach of personal information?

The City determines whether personal information has been accessed to determine what response should be taken. The City's default position is to voluntarily report data breaches to the Privacy Commissioner. If there are good reasons not to do so these will be recorded in the City's internal report of the breach.

The City will determine the seriousness of a breach by:

- considering the type of data held
- whether personal or health information was disclosed
- the number of individuals affected, and
- the risk of harm that could be caused to both individuals and the City by the breach.

After the seriousness of a breach has been determined, the City will take the following steps to manage a data breach:

Contain – steps will be taken to contain the breach and minimise any resulting damage.

Evaluate – the type of data involved in the breach will be assessed, and the risks associated with the breach, to determine next steps. This will include an assessment of who is affected by the breach, what was the cause of the breach, and any foreseeable harm to the affected individuals/organisations.

Notify – individuals/organisations affected by the breach will be notified as soon as possible to enable them to take any steps required to protect themselves, and to advise them of their rights to lodge a complaint with the Privacy Commissioner. The City's default position is to voluntarily report data breaches of personal information to the Privacy Commissioner.

Act – any additional action identified to mitigate risks will be implemented.

Prevent – preventive efforts will be put into action based on the type and seriousness of the breach.

Review rights and complaints

Internal review

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

Internal review process

Applications for an internal review must be made within **six months** from the date when the applicant first became aware of the breach. Applications must be made in writing and addressed to the City's Privacy Contact Officer. Refer to Appendix A - Privacy complaint: internal review application form.

The Privacy Contact Officer will conduct the internal review unless the internal review is about the conduct of the Privacy Contact Officer. In this case the Director Legal and Governance will appoint another person to conduct the internal review.

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

The City will:

- acknowledge receipt of an internal review within **5 working days**; and
- complete an internal review within **60 calendar days**.

The City's Privacy Contact Officer will inform the applicant of the progress of the internal review and will respond in writing within **14 calendar days** of determining the internal review.

If an applicant is not notified of the outcome of an internal review within 60 days, the applicant may seek an external review.

The Privacy Commissioner's role in internal reviews

The City will notify the Privacy Commissioner of internal reviews. The Privacy Commissioner is entitled to make submissions to the City regarding internal reviews. Noting that an individual can make a complaint direct to the Privacy Commissioner about an alleged breach of their privacy.

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

An applicant may seek an external review by the NSW Civil and Administrative Tribunal

To seek an external review, an application must be made to the NCAT within **28 days** from the date of the internal review determination.



Other ways to resolve privacy concerns

The City encourages the informal resolution of privacy issues before undertaking the review process. Issues can be raised informally with the City. Please refer to the City's [website for contact details](#).

Complaints not dealt with through the internal review process will be managed under the City's Complaints and Feedback Procedures available for download from the City's website.

Promoting privacy

The City reinforces compliance with the PPIP Act and HRIP Act by:

- endorsing this Plan and making it publicly available;
- providing a copy of this Plan to relevant oversight bodies such as the Audit, Risk and Compliance Committee;
- reporting on internal reviews to the Office of the Information and Privacy Commission; and
- identifying privacy issues when implementing new systems, services and processes.

Employee awareness

The City ensures that its employees are aware of and understand this Plan and how it applies to the work they do.

The City promotes awareness of privacy obligations among employees by:

- publishing the City's Privacy Management Plan and privacy-related policies on the City's intranet and website;
- publishing information about privacy on the City's intranet;
- communicating regularly with employees about privacy;
- ensuring City policies comply with privacy legislation;
- including the Plan in induction packs; and
- offering training and advice to employees.

Public awareness

This Plan provides information to members of the public about how the City manages personal and health information. The Plan is publicly available as open access information under the GIPA Act [here](#).

The City promotes public awareness of the City's Privacy Management Plan by:

- publishing the Plan on the City's [website](#);
- providing hard copies of the Plan free of charge on request;
- translating the Plan into other languages and alternative formats on request; and
- informing people about the Plan when responding to enquiries about personal and health information.

Privacy and other legislation

This section contains a general summary of how the City must manage personal and health information under the Privacy and Personal Information Protection Act 1998 (PPIP Act), the Health Records and Information Privacy Act 2002 (HRIP Act) and other relevant laws.

The Privacy and Personal Information Protection Act

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

Information protection principles (IPPs)

Part 2, Division 1 of the PPIP Act contains 12 IPPs the City must comply with. These are:

Collection

The City will:

1. collect personal information only for a lawful purpose that is directly related to the City's functions and activities;
2. collect personal information directly from the person concerned;
3. inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. Also how the personal information can be accessed and amended and any possible consequences of not providing personal information;
4. ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into people's personal affairs.

Storage

5. The City will store personal information securely, keep it no longer than necessary and destroy it appropriately. Personal information is protected from unauthorised access, use or disclosure.

Access and accuracy

The City is:

6. transparent about the personal information it holds, why it is used, and the right to access and amend it;
7. allows people to access their own personal information without unreasonable delay or expense;
8. allows people to update, correct or amend their personal information where it is necessary;
9. endeavors to ensure that personal information is relevant and accurate before using it.

Use

10. The City only uses personal information for the purpose it was collected for unless it has consent for its use for another purpose.

Disclosure

The City:

11. does not disclose personal information without consent, unless disclosure is permitted under the PPIPA or other legislation;
12. does not disclose sensitive personal information without consent, eg ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

Offences

Offences can be found in s62-68 of the PPIPA Act. It is an offence for the City to:

- intentionally disclose or use personal information for an unauthorised purpose;
- offer to supply personal information that has been disclosed unlawfully;
- hinder the Privacy Commissioner or their employees from doing their job.

The Health Records and Information Privacy Act

The HRIP Act sets out how the City must manage **health** information.

Health privacy principles (HPPs)

Schedule 1 of the HRIP Act contains 15 HPPs that the City must comply with. These are:

Collection

The City:

1. collects health information only for a lawful purpose that is directly related to the City's functions and activities;
2. ensures that health information is relevant, accurate, is not excessive and does not unreasonably intrude into people's personal affairs;
3. collects health information directly from the person concerned or with consent from the person concerned;
4. informs people why their health information is being collected, what it will be used for, and to whom it will be disclosed. Also how it can be accessed and amended and any possible consequences of not providing health information.

Storage

5. The City stores health information securely, keeps it no longer than necessary and destroys it appropriately. Health information is protected from unauthorised access, use or disclosure.

Access and accuracy

The City is:

6. transparent about the health information it holds, why it is used, and the right to access and amend it;
7. allows people to access their own health information without unreasonable delay or expense;

8. allows people to update, correct or amend their health information where necessary;
9. ensures that health information is relevant and accurate before using it.

Use

10. The City only uses health information for the purpose it was collected for unless it has consent for its use for another purpose.

Disclosure

11. The City does not disclose personal information without consent, unless disclosure is permitted under the HRIPA or other legislation;

Identifiers and anonymity

The City:

12. may use unique identifiers for health information;
13. allows people to remain anonymous where it is lawful and practicable.

Transfers and linkage

The City:

14. does not transfer health information outside of NSW;
15. does not currently use a health records linkage system.

Offences

Offences can be found in s68-70 of the HRIP Act. It is an offence for the City to:

- intentionally disclose or use health information for an unauthorised purpose;
- offer to supply health information that has been disclosed unlawfully.

Other relevant laws

This section contains information about other relevant legislation.

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

Under this Act and Regulation people can apply for access to information held by the City. This information may include personal or health information.

Independent Commission Against Corruption Act 1988

Under this Act the City must provide information to the Independent Commission Against Corruption about allegations of fraud and corruption that may contain personal information.

Public Interest Disclosures Act 1994 (PID Act)

Under the PID Act people working for a NSW public sector agency can make a public interest disclosure to the City.

The PID Act requires that information that might identify or tend to identify a person who has made a public interest disclosure should be protected.

State Records Act 1998 and State Records Regulation 2010

This Act and Regulation authorise the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.

City of Sydney Act 1988

This Act requires the City to collect personal information to maintain the non-residential register of electoral information.

Referrals to external agencies under other relevant legislation

Under the *Ombudsman Act*, the *Independent Commission Against Corruption Act 1998*, and the *Crimes Act 1900* the City can provide information to the:

- NSW Ombudsman;
- Independent Commission Against Corruption; and
- NSW Police.

Exemptions, directions and codes of practice

Exemptions to the Information Protection Principles (IPPs)

Part 2, Division 3 of the PPIP Act contains exemptions that may permit the City not to comply with IPPs in certain situations. These include the following:

- the City is not required to comply with IPPs 2-3, 6-8, or 10-12 if lawfully authorised or required not to do so;
- the City is not required to comply with IPP 2 if the information concerned is collected in relation to court or tribunal proceedings.

Exemptions to the Health Privacy Principles (HPPs)

Exemptions are located mainly in Schedule 1 to the HRIP Act, and may permit the City not to comply with HPPs in certain situations. For example, the City is not required to comply with HPPs 4-8, and 10 if lawfully authorised or required not to do so.

Privacy codes of practice

The City has adopted the Privacy Code of Practice for Local Government as prepared by the Office of the Privacy Commissioner and the Health Records and Information Privacy Code of Practice 2005.

Under the Privacy Code of Practice for Local Government where it is reasonably necessary, the City may indirectly collect and use personal information to confer an award, prize, or similar form of personal recognition on the person about whom the information relates.

The Privacy Code of Practice for Local Government also permits the City to use personal information for a purpose other than the purpose for which it was collected where the use is in pursuance of the City's lawful and proper functions and the personal information is reasonably necessary for the exercise of those functions. In general, the City does not use personal information for a purpose other than which it was collected without the consent of the individual.

Contact details

Further information about the City's Privacy Management Plan, or the personal and health information the City holds can be obtained from the City's Privacy Officer:

Telephone: 02 9265 9333

Hearing/speech impaired:

- 133677 TTY/voice calls
- 1300 555 727 Speak & Listen
- 0423 677 767 SMS relay

Fax: 02 9265 9222

Email: governance@cityofsydney.nsw.gov.au

Street address

Town Hall House
Level 2, 456 Kent Street
Sydney NSW 2000

Postal address

City of Sydney
GPO Box 1591
Sydney
NSW 2001

Contact details for the Office of the Information and Privacy Commissioner are:

Email: ipcinfo@ipc.nsw.gov.au

Telephone: 1800 472 679

Interpreter Service: 131 450

Street/Postal address:

Level 17, 201 Elizabeth Street
Sydney NSW 2000

Contact details for the NSW Civil and Administrative Tribunal are:

Telephone: 1300 006 228

Interpreter Service: 13 14 50

National Relay Service: 1300 555 727

Street/Postal address:

John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000

Approval

Approval status

The Chief Executive Officer approved this policy on 20/02/2019



Kim Woodbury, ACEO

20 February 2019

Approval history

Stage	Date	Comment	TRIM Reference
Original policy	16 October 2013	Endorsed by the Executive	2013/405028
Review	February 2019	Data breach information and Appendix A added, and minor amendments made	2019/105539
Next review	February 2021		

Ownership and approval

Responsibility	Role
Author	Manager Risk & Governance
Owner	Director Legal & Governance
Endorser	City of Sydney Executive
Approver	Chief Executive Officer

APPENDIX A



Privacy complaint: internal review application form

This is an application¹ for review of conduct under: (please select one)
 s53 of the Privacy and Personal Information Protection Act 1998 (PPIP Act)
 s21 of the Health Records and Information Privacy Act 2002 (HRIP Act)

1	Your full name:
2	Your postal address: Telephone number: Email address:
3	If the complaint is on behalf of someone else, please provide their details: What is your relationship to this person (eg. parent)? Is the person capable of making the complaint by himself or herself? <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> unsure
4	What is the specific conduct ³ you are complaining about? <i>(see footnote for explanation of "conduct")</i>
5	Please tick which of the following describes your complaint: <i>(you may tick more than one option)</i> <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
6	When did the conduct occur (date)? <i>(please be as specific as you can)</i>

7	When did you first become aware of this conduct (date)?
8	You need to lodge this application within six months of the date at Q.7. If more than six months has passed, you will need to ask the City for special permission to lodge a late application. Please explain why you have taken more than six months to make your complaint (<i>for example: 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</i>):
9	What effect did the conduct have on you?
10	What effect might the conduct have on you in the future?
11	What would you like to see the City do about the conduct? (<i>for example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.</i>)

I understand that this form will be used by the City of Sydney 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 *Privacy and Personal Information Protection Act*; or section 21 of the *Health Records and Information Privacy Act*; and that the Privacy Commissioner will be kept advised of the progress of the internal review.

Your signature: _____

Date:

SEND THIS FORM TO: governance@cityofsydney.nsw.gov.au

Keep a copy for your records.

For more information on the PPIP Act or the HRIP Act visit: www.ipc.nsw.gov.au

-
- 1 It is not a requirement under the PPIP 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 City of Sydney for the matter to be a valid internal review.
 - 2 The PPIP Act regulates NSW state government departments, area health services, most other state government bodies, and NSW local councils. Each of these is defined as a “public sector agency”. The HRIP Act regulates private and public sector agencies and private sector persons.
 - 3 “Conduct” can include an action, a decision, or even inaction by the City of Sydney. 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.
-