CITY OF SYDNEY

Privacy Management Plan

Privacy Management Plan
September 2026

The City of Sydney acknowledges the Gadigal of the Eora Nation as the Traditional Custodians of our local area.

Contents

Introduction	3
About the City	3
What is personal and health information	4
How the City collects and manages personal and health information	5
Public registers	11
How to access and amend personal and health information	11
Data breaches	12
Review rights and complaints	12
Promoting privacy	14
Managing personal and health information under legislation	15
Laws and Standards	19
Related City of Sydney Policies and Procedures	20
Consultation	21
Contact details	21
Review period	22
Approval status	22
Approval history	22
Ownership and approval	23

Introduction

The purpose of this Privacy Management Plan (Plan) is to explain how the City of Sydney (the City) manages personal and health information in accordance with NSW privacy laws. This includes the:

- Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)
- Health Records and Information Privacy Act 2002 (NSW) (HRIP Act).

This Plan also explains who our community should contact about the personal and health information collected and held by the City, how the information can be accessed and amended and how privacy complaints are handled. Additionally, this Plan is used to guide the City's employees in how to deal with personal and health information.

What this Plan covers

The City is required to have a Plan under s33 of the PPIP Act which must include:

– information about how the City develops policies and practices to ensure compliance with the PPIP Act and the HRIP Act

– how people within the City are made aware of these policies and practices

– the City's internal review procedures

– anything else the City considers relevant to the Plan in relation to privacy and the personal and health information it holds.

Any reference to employees in this Plan includes permanent (whether full-time or part-time), temporary and casual employees together with agency contractors, consultants, volunteers, trainees and apprentices, and students on work placements.

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 City of Sydney Act 1988, 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.

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 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 manage, improve and develop resources available to the community.

More detailed information is available on the City's website.

What is personal and health information

Personal information

Personal information is defined in s4 of the PPIP Act as any information or opinion about a person where that person's identity is apparent or can be reasonably ascertained from the information or opinion.

Personal information can include, for example, a person's name, personal address and contact details, information about their family life, their sexual preferences, financial information, biometric information and photos.

What is not personal information under the PPIP Act?

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.

The Privacy and Personal Information Protection Regulation 2019 also lists other information that is not personal information, such as information about someone that is contained in:

– a document in a library, art gallery or museum
– State records under the control of the State Archives and Records Authority of New South Wales
– public archives (within the meaning of the Copyright Act 1968 (Cth)).

The City Archives is a public archive within the meaning of the Copyright Act. The access directions issued by the City under Part 6 of the State Records Act 1998 determine when information in the City Archives can be released to the public. For example, information about an individual contained in a development application may be released via the City Archives 10 years after the file is closed.

Health information

Health information is a more specific type of personal information and is defined in s6 of the HRIP Act.

Health information includes information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided to a person.

Examples of health information include healthcare identifiers, 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

The City is committed to building good privacy practices into its decision making, as well as the design and structure of its information systems, business processes and services.

The City considers privacy at all stages of initiatives, from conception through to the development and implementation phase and is committed to developing an organisation-wide awareness of privacy and supporting the principles of data minimisation and informed consent.

Management of information at the City, including personal and health information, is governed by our Records Management Policy, Information Protection Policy and associated procedures.

Collection of personal and health information

The City collects personal and health information in a variety of ways in order to perform services and functions. The City assesses the level of personal information that is appropriate to be collected on a case-by-case basis with a view to minimising the amount of personal and health information it collects and manages.

The City supports this commitment through a range of tools including organisation wide training on this Plan and our privacy requirements including a commitment to data minimisation, detailed guidance on our intranet privacy pages and advice from Governance on individual privacy protection notices and privacy requirements.

The City takes active steps to make sure the information it collects is relevant, accurate, complete, up to date and not excessive. Steps include collecting the information directly from the individual wherever possible, reconfirming details, regularly reviewing information collection processes and maintaining up to date and synchronised databases. The City is committed to only collecting the minimum amount of personal information necessary for each specified purpose.

Personal and health information may be collected from:

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

Contractors acting on the City's behalf may also collect personal and health information. The City endeavours to include clauses in its contracts that require contractors to comply with relevant privacy obligations, where commercially appropriate. Where the City is entering into contracts with a third party supplier using terms or contracts supplied by that third party supplier, the City undertakes a due diligence as to the third party supplier's management of personal information and based on the outcome of the due diligence, takes all steps necessary to ensure that the personal information is managed in accordance with principles similar to the principles set out in the PPIP Act.

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

– levying and collecting rates
– providing services, for example, childcare, libraries, pet registration 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
– recruitment and employment
– fitness for work
– requests for service, for example, asset repair, booked collections and street cleansing.

Personal and health information may be collected by the City in many ways including:

– incident reports
– medical assessment reports
– immunisation history statements
– submissions
– application forms
– CCTV footage
– public registers
– financial transaction records
– contracts
– customer enquiries
– telematics
– online services
– images, video footage and/or audio recordings from City events

– annual disclosure of interests declarations
– event registrations
– contact tracing under NSW Public Health Orders.

Personal and health information may be collected electronically, in writing, over the telephone and in person. The City's telephone system displays the number of the person who called, except for private/silent numbers, and can identify through this number any related customer records. Telephone calls may be electronically recorded for training and quality assurance purposes and callers are provided with an opt-out option.

The City will allow people to remain anonymous where it is lawful and practicable. For example, where possible our online surveys and other community engagement initiatives allow for feedback to be given anonymously.

The City will not collect personal information from third parties unless the individual has authorised collection from someone else or, in the case of information relating to a person under the age of 16 years, the information has been provided by a parent or guardian. For example, from a parent or guardian about a child attending a City program.

The City will collect health information about an individual only from that individual, or with consent from the person concerned, unless it is unreasonable or impracticable to do so.

Personal and health information provided to the City

Individuals may provide the City with personal or health information, for example when they make an application for employment, request a service, make enquiries or enrol in a program. This can include names, contact details, opinions, details concerning an individual's physical or mental health, family relationships, housing or tenancy information, financial information, work and education details. Individuals may also provide the City with personal information about other people, for example when they make a complaint.

Identity verification

Individuals may provide the City with documents to verify their identity, for example a driver licence when they make an application for a parking permit or busking permit. Where possible the City will not retain copies of personal identity documents. State Records NSW provides authorisation to the effect that copies of records used to verify the identity of a customer or collected as part of a recruitment process can be retained until verification or validation process has been completed and then destroyed. This approach is supported by organisational procedures and record management reviews.

Unsolicited information

Unsolicited information is personal or health information received by the City in circumstances where the City has not asked for or required the information to be provided. Such information is not deemed to have been collected by the City but the access, storage, use and disclosure Information Protection Principles and Health Privacy Principles in this Plan will apply to any such information that is retained by the City.

Privacy Protection Notice

Under Information Protection Principle 3 and Health Privacy Principle 4, when the City collects personal or health information from an individual, such as their name, address, telephone number or email address or information about their physical or mental health or disability, the City must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual is made 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
– the name and address of the agency that is collecting the information and the agency that is to hold the information (the City is a public sector 'agency' under s10 of the PPIP Act).

To ensure the City complies with the PPIP Act and HRIP Act, a **Privacy Protection Notice** will be included on/in all City forms, letters, documents and other records (e.g. electronic, digital) that request and/or collect personal and/or health information from individuals.

City employees are encouraged to consult with the City's Governance team to confirm that each Privacy Protection Notice is fit for purpose and complies with the City's privacy requirements. The City's Governance team provides guidance on and reviews draft Privacy Protection Notices at the City for consistency, accuracy and compliance with the PPIP Act's Information Protection Principles.

The City's Privacy Protection Notice template

PRIVACY PROTECTION NOTICE

Purpose of collection: This information is being collected to (s*pecify the purpose(s) for which the information is being collected e.g. provide a community program and service)*.

Intended recipients: City of Sydney employees (*and specifically list any other organisations/outsourced service providers e.g. arborists, NSW Health etc.)*

Supply: The supply of this information (is required by law **or** is voluntary – *delete one)* If you are unwilling to provide this information, the City of Sydney may be unable to provide access to City of Sydney services.

Access/Correction: Please contact Customer Service on 02 9265 9333 or at council@cityofsydney.nsw.gov.au to access or correct your personal information.

Storage: The (*insert name of business unit*) at the City of Sydney, located at 456 Kent Street, Sydney NSW 2000*,* is collecting this information and the City of Sydney will store it securely.

Other uses: The City of Sydney will use your personal information for the purpose for which it was collected and may use it as is necessary for the exercise of other functions. Other uses may include *(specify other reasonably necessary uses if any and include opt out or opt in check boxes where possible or delete this second sentence).*

[Note: Health information cannot be used for a secondary purpose unless the individual has consented to this other use or it is directly related to the primary purpose. Delete Other uses paragraph if collecting health information.]

For further details on how the City of Sydney manages personal information, please refer to our Privacy Management Plan (https://www.cityofsydney.nsw.gov.au/policies/privacy-management-plan).

Note: An 'opt out' or 'opt in' check box should be provided for 'Other uses' where possible.

Storage, access and accuracy of personal and health information

Personal information and health information are both sensitive information and are stored electronically and in hard copy files. The preference for storage of personal information is in Australia and if it is necessary to store personal information outside of Australia, then an appropriate risk assessment is undertaken prior to this decision being made. If any data containing personal information is stored outside of Australia, then it is carefully managed to ensure that it is protected appropriately.

However, it is noted health information is stored in NSW in accordance with Health Privacy Principle 14 unless the conditions under Health Privacy Principle 14 are met, such as individual consent.

The following applies to information the City holds:

– only authorised City employees and authorised third parties can access personal information
– employees will take reasonable steps to ensure personal information is accurate before using it
– a person may access or request the amendment of personal and health information the City holds about them by contacting the City's Customer Service
– personal information will be kept no longer than necessary (as defined in the purpose and other uses in the PPN) and disposed of appropriately in accordance with the City's Records Management Policy.

Reasonable steps to ensure accuracy include collecting the information directly from the individual wherever possible, reconfirming details and maintaining up to date databases.

Please refer to Managing personal and health information under legislation below for details of exemptions, directions and codes of practice that may affect the above.

Electronic information will be stored on secure information systems that require individual logins. A user must be authenticated each time they attempt to log onto the City's network or systems. Authorised staff are responsible for the security of their passwords and accounts. In addition the City's record management system allows for access controls to be applied to ensure only authorised staff can access sensitive information. New systems will be assessed for compliance with the PPIP Act and HRIP Act. Hard copy files and sensitive information will also be securely stored.

Use and disclosure of personal and health information

The City will use your personal information for the purpose for which it was collected and may use it as is necessary for the exercise of other council functions where it is satisfied that the personal information is reasonably necessary for the exercise of such functions.

For example, your personal information may be used to understand community and customer needs to improve our services. The City may also use your information to let you know about services or other information available (e.g. newsletters) and may share your information within other divisions of the City and authorised outsourced service providers to expedite services to customers.

Employees use the personal information collected to:

– deliver services
– conduct research
– provide advice
– continually improve services.

The City is committed to anonymise (de-identify) data kept for long-term business intelligence purposes.

The City will only use health information for the purpose it was collected for unless it has consent for its use for another purpose, the secondary purpose is directly related to the primary purpose or it is permitted under legislation, such as an emergency or serious threat to health or welfare.

The City does not disclose personal or health information without consent, unless the disclosure is:

– for a purpose directly related to the reason the City collected it, and the City has no reason to believe the individual would object,
– necessary to prevent or lessen a serious and imminent threat to someone's life or health, or
– permitted under the PPIP Act, the HRIP Act or other legislation.

The City will not disclose personal information relating to a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities without consent, unless such disclosure is necessary to prevent or lessen a serious and imminent threat to life or health or is required by law.

Use of Artificial Intelligence (AI)

The City has a procedure that provides direction to City employees on the appropriate use of this technology, including generative AI tools. Employees are permitted to use an approved AI tool, Microsoft Copilot, by logging in through their work email address which ensures commercial data protection.

Privacy and data protection is prioritised. The procedure prohibits employees from entering any personal, health information or confidential information into any generative AI tool. The procedure provides guidance to staff when engaging with third party providers and if appropriate, terms can be incorporated as part of the contract terms.

Employees can only use generative AI in low-risk situations. It is not a substitute for an employee's judgement or accountability. Examples of supported uses of AI tools include building an initial outline for a policy or PowerPoint presentation, developing a project plan, writing a first draft of correspondence using plain English principles, summarising text from a lengthy public report or draft a post for a website.

The City reviews requests for custom or configured generative AI tools or instances on a case by case basis, including a use case assessment regarding risk profile, technical feasibility and viability. Examples of the limited supported initiatives to date include a chatbot that helps employees locate information from within the City's Sharepoint intranet and an internal Pathway bot that assists some staff on the use of a particular platform.

The procedure is reviewed at least every year. As this is an emerging technology the City actively monitors and reviews our use of Artificial Intelligence to ensure our ongoing compliance with the Information Protection Principles.

Use of Automated Decision Making

The City of Sydney does not use any fully automated decision making technical systems. City employees are accountable for all statutory decisions made by the City. No final decisions are made without human input.

Some systems used by the City may have partially automated or rules-based functions embedded that may assist with a preliminary step in the decision-making process. For example, a function within the City's recruitment system identifies through a screening question, applicants who do not meet the essential selection criteria for particular positions at the City that require a driver licence. In this case, the application is retained but it is moved to the unsuccessful step in the workflow, and

an outcome email is generated. This outcome email includes a contact point to allow an individual to challenge the decision or seek reconsideration.

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 disclosing 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:

- Contracts over $150,000 awarded by the City
- Data breach notification register
- Development contributions register
- Land register
- Non-residential roll and roll of occupiers and ratepaying lessees.
- Public record of licences
- Record of building certificates
- Record of impounding
- Register of councillor meetings with registered lobbyists and property developers
- Register of political donation disclosures
- Register of development consents
- Register of pecuniary interest declarations
- Register of investments
- Register of planning agreements

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.

If you wish to access or amend your personal and/or health information the City holds such as your contact details please contact the City's Customer Service, complete our on-line form or on 02 9265 9333. We will direct your enquiry to the applicable area of the organisation or the City's Privacy Officer. If necessary, the City will seek verification of your identity. The City does not charge a fee to access and amend personal and health information.

If you have a City Connect Account you can log in to access your requests and applications lodged through your account, for example, allocated parking permits, property titles, your rate payments and property certificate purchase information.

Accessing or amending other people's information

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

– under s26 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 s7 and s8 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, in order to help find a missing person or for compassionate reasons.

Data breaches

Separate from this Plan the City's Data Breach Policy provides guidance on how the City responds to data breaches of City held information. It sets out the procedures for managing a data breach, including the assessment and notification requirements for the Mandatory Notification of Data Breach Scheme under the PPIP Act.

A data breach occurs when there is a failure that has caused unauthorised access to, or unauthorised disclosure of, data held by the City.

Review rights and complaints

The City encourages the informal resolution of privacy issues before undertaking the internal review process. Issues can be raised informally with the City and managed under the City's Complaint Management Policy. Further details on how the City manages complaints can be found on the City's website.

Internal review

Individuals have the right to seek an internal review under Part 5 of the PPIP Act if they believe 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.

An internal review is an internal investigation that the City conducts into a complaint. The City will assess whether or not it has complied with its privacy obligations, and then tell the applicant of its findings and if it will take any further action.

Applications for an internal review

Applications for an internal review must:

– be in writing

– be addressed to the City (our key contact is the Privacy Contact Officer Executive Manager Risk and Governance)
– specify a postal or email address in Australia to which the City may send its review response
– be made within six months from first becoming aware of the conduct that is the subject of the application.

The City recommends that applicants use the Information and Privacy Commission's Privacy Complaint: Internal Review Application Form when submitting a written request for a review with the City.

Internal review process

The Privacy Contact Officer or their delegate will conduct the internal review. If the internal review is about the conduct of the Privacy Contact Officer, the Executive Director Legal & Governance will appoint another person to conduct the internal review.

The Privacy Contact Officer will refer to the Privacy Commissioner's guidance materials including the IPC Checklist: How to handle an Internal Review when carrying out an internal review.

The City aims to:

– acknowledge receipt of an internal review within **5 working days**
– complete an internal review within **60 calendar days**.

Once the review is completed, the City may take no further action, or it may do one or more of the following:

– make a formal apology
– take remedial action
– provide undertakings that the conduct will not occur again
– implement administrative measures to reduce the likelihood of the conduct occurring again.

The City's Privacy Contact Officer will notify the applicant in writing within 14 days of completing an internal review of:

– the findings of the review
– the action proposed to be taken by the City and the reasons for taking that action (if any)
– the right of the applicant to have those findings, and the City's proposed action, administratively reviewed by the NSW Civil and Administrative Tribunal.

The Privacy Commissioner's role in internal reviews

The Privacy Commissioner has an oversight role in how agencies handle privacy complaints and is entitled to make submissions to the City regarding internal reviews.

If the City receives an internal review application, it will:

– notify the Privacy Commissioner of the application as soon as practicable after receiving the application
– keep the Privacy Commissioner informed of the progress of the internal review

– inform the Privacy Commissioner of the findings of the review and any action proposed to be taken by the City in relation to the matter.

An individual can also make a complaint directly to the Privacy Commissioner about an alleged breach of their privacy.

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

If an internal review is not completed within 60 days, or the applicant is not satisfied with the findings of an internal review or the action taken by the City in relation to the review, the applicant has 28 days to apply to NCAT to review the conduct or decision complained about. NCAT's role is to assess whether or not the City complied with its privacy obligations.

Promoting privacy

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

– endorsing this Plan and making it publicly available on its website

– providing a copy of this Plan to relevant oversight bodies such as the Audit, Risk and Compliance Committee

– reporting on internal reviews to the Privacy Commissioner

– identifying privacy issues when implementing new systems, services and processes

– conducting ongoing reviews of 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, so that they understand what their privacy obligations are, how to manage personal and health information in their work and what to do if they are unsure.

The City promotes awareness of privacy obligations among employees by:

– publishing this Plan and information about privacy on the City's intranet and website, including our privacy guidelines for employees which are a practical overview of the IPPs and HPPs and their responsibilities

– communicating regularly with employees about privacy

– ensuring City policies comply with privacy legislation through policy authors consulting with the City's Information Protection Coordination Group (IPCG) and Legal & Governance Division

– including the Plan and privacy guidance in the City's new starter induction training

– providing refresher training

– providing targeted advice to employees and business units

– highlighting and promoting the Plan at least annually, during Privacy Awareness Week.

When employees have questions about how to manage personal and health information under this Plan, they may consult with their manager, the Privacy Contact Officer (Executive Manager Risk and Governance) or the Governance team.

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.

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
- referring to the Plan in its privacy notices
- informing people about the Plan when responding to enquiries about personal and health information.

Managing personal and health information under 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 Privacy and Personal Information Protection Regulation 2019, the Health Records and Information Privacy Act 2002 (HRIP Act) and other relevant legislation.

The Privacy and Personal Information Protection Act

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

Information protection principles

Part 2, Division 1 of the PPIP Act contains 12 Information Protection Principles (IPPs) with which the City must comply. The following is an overview of the principles as they apply to the City.

Collection

1. The City collects personal information only for a lawful purpose that is directly related to the City's functions and activities and necessary for that purpose.
2. The City collects personal information directly from the person concerned. The City will not collect personal information from third parties unless the individual has authorised collection from someone else or, in the case of information relating to a person under the age of 16 years, the information has been provided by a parent or guardian.
3. The City informs people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. The City will tell people how they can access and amend their personal information and any possible implications if they decide not to give their personal information to us.
4. The City ensures that personal information is relevant, accurate, complete, up to date and 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 dispose of it securely and in accordance with the City's obligations under the State Records Act 1998 and any other requirements for the retention and disposal of personal information. Personal information is protected from unauthorised access, use or disclosure.

Access and accuracy

6. The City is transparent about the personal information it holds, why it is used, and the right to access and amend it.
7. The City allows people to access their own personal information without unreasonable delay or expense.
8. The City allows people to update, correct or amend their personal information where it is necessary.

Use

9. The City will take reasonable steps to ensure that personal information is relevant ,accurate, up to date and complete before using it.

10. The City only uses personal information for:
    a. the purpose for which it was collected and directly related purposes
    b. to prevent or lessen a serious or imminent threat to the life or health of the individual to whom the information relates or of another person
    c. other purposes as specified under 'Exemptions and the Privacy Code of Practice for Local Government' below, or
    d. any other purpose only with consent.

Disclosure

11. The City does not disclose personal information without consent, unless disclosure is:
    a. for a purpose directly related to the reason we collected it, and where the City has no reason to believe the individual would object
    b. necessary to prevent or lessen a serious and imminent threat to someone's life or health, or
    c. permitted under the PPIP Act, Privacy Codes of Practice under the PPIP Act or the HRIP Act or other legislation.
12. The City does not disclose sensitive personal information without consent, e.g. ethnicity or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership, unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

Exemptions and the Privacy Code of Practice for Local Government

1. Exemptions to the Information Protection Principles (IPPs)

Part 2, Division 3 of the PPIP Act contains exemptions that may permit the City to not 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
– the City is not required to comply with IPPs 1-4, 10 or 11 in relation to emergency situations

– the City is not required to comply with IPPs 1-4, 10 or 11 if the City is providing the information to another public sector agency, in particular to enable inquiries to be referred between the agencies concerned.

For example, s 23(3) of the PPIP Act provides that the City is not required to comply with collection requirements if the information concerned is collected for law enforcement purposes such as the issue of a penalty infringement notice.

2. Privacy Code of Practice for Local Government

The City must comply with the Privacy Code of Practice for Local Government as prepared by the Office of the Privacy Commissioner and revised on 20 December 2019.

a. 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.

b. 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 City is satisfied that the personal information is reasonably necessary for the exercise of those functions.

   For example, the Rates Record that the City holds under s602 of the Local Government Act 1993 may be used to:

   – notify neighbours of a proposed development
   – evaluate a road opening or
   – evaluate a tree preservation order.

   In addition, the City may use personal information for other specific purposes where the City is satisfied that the information is reasonably necessary for another function such as:

   – understanding community and customer needs to improve our services
   – letting customers know about services or other information available (e.g. newsletters)
   – sharing personal information within other divisions of the City and authorised outsourced service providers to expedite services to customers.

Offences

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

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

When dealing with personal information the City's Code of Conduct requires council officials to comply with:

– the PPIP Act and HRIP Act
– the Information Protection Principles and Health Privacy Principles
– this Plan

– the Privacy Code of Practice for Local Government.

All council officials receive training in the City's Code of Conduct. Breaches of the Code of Conduct may lead to disciplinary action up to and including termination of employment.

The Health Records and Information Privacy Act

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

Health privacy principles

Schedule 1 of the HRIP Act contains 15 Health Privacy Principles ('HPPs') that the City must comply with. The following is an overview of the principles as they apply to the City.

Collection

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

Storage

5. The City stores health information securely, keeps it no longer than necessary and destroys it securely and in accordance with the City's obligations under the State Records Act 1998 and any other requirements for the retention and disposal of personal information. Health information is protected against loss, unauthorised access, use, modification, disclosure or any other misuse.

Access and accuracy

6. The City is transparent about the health information it holds, why it is used, and the right to access and amend it.
7. The City allows people to access their own health information without unreasonable delay or expense.
8. The City allows people to update, correct, delete, add or amend their health information where necessary.
9. The City ensures that health information is relevant and accurate before using it.

Use

10. The City only uses health information for the purpose for which it was collected, or a directly related purpose that you would expect, unless it has consent for its use for another purpose, or one of the exemptions in HPP 10 (noted below) applies.

Disclosure

11. The City only discloses health information for a purpose for which it was collected, or a directly related purpose that you would expect, unless it has consent for its disclosure for another purpose, or one of the exemptions in HPP 11 (noted below) applies.

Identifiers and anonymity

12. The City does not use unique identification numbers (identifiers) for health information, as they are not needed to carry out our functions.
13. The City allows people to remain anonymous where it is lawful and practicable.

Transfers and linkage

14. Unless otherwise stated in this plan, the City does not transfer health information outside of NSW.
15. The City does not currently use a health records linkage system.

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 10-11 if lawfully authorised or required not to do so.

For example, the City may disclose health information to assist in a stage of an emergency, in the event of a serious and imminent threat to the life, health and safety of the individual or another person or a serious threat to public health or public safety to find a missing person or for compassionate reasons.

Health Records and Information Privacy Code of Practice 2005

The Health Records and Information Privacy Code of Practice 2005 applies to the City. It permits, in certain limited circumstances, the collection, use and disclosure of health information between human services agencies without the consent of the person to whom the health information relates. A human services agency is a public sector agency that provides welfare services, health services, mental health services, disability services, drug and alcohol treatment services, housing and support services and/or education services.

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.

Laws and Standards

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

A request for City records may be made through the City's website.

Under this Act and Regulation members of the public can apply for access to information held by the City. This information may include personal or health information. If the personal or health information is about a third party rather than the applicant, the GIPA Act requires that the City take all reasonable steps to consult with the third party to ensure their information is not released without proper consultation and careful consideration.

City employees - name and position title

Schedule 4 of the GIPA Act also provides that information about a City employee, including their name and non-personal contact details (such as position title and their public functions at the City) is not personal information for the purposes of the GIPA Act.

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 and/or health information.

Public Interest Disclosures Act 2022 (PID Act)

Under the PID Act any public official can make a public interest disclosure to the City.

The PID Act requires that information tending to identify a person who has made a public interest disclosure is not to be disclosed by a public official or the City.

Section 64(2) of the PID Act includes exceptions to this requirement, including if the person consents in writing to the disclosure of the identifying information, it is generally known the person is the maker of the public interest disclosure due to their voluntary self-identification, the City reasonably considers it necessary, after consultation, to disclose the identifying information to protect a person from detriment or it is necessary that it be disclosed to a person whose interests are affected by the disclosure.

State Records Act 1998 and State Records Regulation 2024

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.

Referrals to external agencies under other relevant legislation

Under the Ombudsman Act 1974, the Independent Commission Against Corruption Act 1998, and the Crimes Act 1900, the City can provide information, including personal and health information, to the:

– NSW Ombudsman

– Independent Commission Against Corruption

– NSW Police.

Related City of Sydney Policies and Procedures

- Access to Information Policy
- Code of Conduct
- Compliance Obligations Policy (internal policy)
- Complaint Management Policy

- Data Breach Policy
- Generative AI Procedure
- Information Protection Policy
- IT Products and Services Acquisition, Management and Retirement Policy (internal policy)
- IT Projects Governance Policy (internal policy)
- IT Systems Security Policy
- Records Management Policy
- Telematics Policy (internal policy)
- Privacy guidelines for employees (internal guidelines)

Consultation

In preparing this updated Plan, Governance consulted with the City's Information Protection Coordination Group (IPCG), Executive Manager Service Experience, People & Culture and Legal Services. They reviewed this Plan and provided comments.

Contact details

Further information about the City's Privacy Management Plan, the personal and health information the City holds and our use of Artificial Intelligence and Automated Decision-Making systems can be obtained from the City's Privacy Contact Officer.

Privacy Contact Officer – Executive Manager Risk & Governance

Email:	governance@cityofsydney.nsw.gov.au
Telephone**:**	02 9265 9333
Address:	Town Hall House, Level 2, 456 Kent Street, Sydney NSW 2000
Postal:	City of Sydney, GPO Box 1591, Sydney NSW 2001
Website:	https://www.cityofsydney.nsw.gov.au/

People with disability: If you're deaf, hard of hearing or have a speech impairment, you can contact us through the National Relay Service. You'll need to provide our phone number, 02 9265 9333.

Information and Privacy Commission

Email:	ipcinfo@ipc.nsw.gov.au
Telephone:	1800 472 679
Address:	Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000
Postal:	GPO Box 7011, Sydney NSW 2001
Website:	https://www.ipc.nsw.gov.au/

NSW Civil and Administrative Tribunal

Email:	aeod@ncat.nsw.gov.au
Telephone:	1300 006 228
Address:	Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000
Postal:	PO Box K1026, Haymarket NSW 1240
Website:	https://www.ncat.nsw.gov.au/

Review period

This Plan will be reviewed every two years.

Approval status

The Chief Executive Officer approved this policy on 24 September 2026.

Emma Rigney, Acting Chief Executive Officer

Approval history

Stage	Date	Comment	TRIM Reference
Original Policy	12 July 2004	Endorsed by CEO	2009/111108
Reviewed	2 October 2013	Reviewed to incorporate the provisions of the Division of Local Government Privacy Management Plan template.	2013/405028
Reviewed	20 February 2019	Data breach information and Appendix A added, and minor amendments made.	2019/048250
Reviewed	18 August 2020	Extensive review including amendment of Privacy Protection Notice and clarification of scope of use exemption.	2020/213654
Reviewed	17 August 2022	Updated in response to recommendations from the IPC and to further clarify and provide guidance. Removed detailed content on data breaches directing employees to the Data Breach Policy.	2020/213654
Reviewed	22 August 2024	Key changes include adding information related to identity verification, the requirement in the Code of Conduct to comply with	2020/213654

Stage	Date	Comment	TRIM Reference
		the PPIPA and HRIPA, and the Mandatory Notification of Data Breach Scheme.	
Reviewed	24 September 2026	Key changes include adding information related to our use of Artificial Intelligence, automated decision making and the risk assessment process undertaken if storing information outside of Australia.	2020/213654
Commence Review Date	24 December 2027		
Approval Due Date	24 September 2028		

Ownership and approval

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