



On Exhibition

PUBLIC NOTIFICATION

Review of Privacy Management Policy & Plan

At the Ordinary Meeting of Council held 28 July 2026 it was resolved that the Privacy Management Policy and draft Privacy Management Plan be placed on public exhibition for 28 days. Council is required to notify the public and provide the opportunity for submissions regarding these documents.

The Privacy Management Policy and draft Privacy Management Plan may be viewed at the Council Chambers, 1 Benerembah Street Griffith, the Griffith City Library and on Council's website.

Anyone wishing to make comment on the draft documents can do so in writing addressed to the General Manager, Griffith City Council, PO Box 485, GRIFFITH NSW 2680 or visit connect.griffith.nsw.gov.au to provide an online submission.

Submissions received will be included in a report to be presented to an Ordinary Meeting of Council. As such, copies of all submissions (including the writer's name and address) will form part of Council's Business Paper and be available to the public. Should you wish to have your contact details withheld it is recommended that you request this in your submission.

Comments or submissions will be received up to **4.00 pm, 27 August 2026.**

CLAUSE **CL08**

TITLE **Review of Privacy Management Policy and Plan**

FROM **Shireen Donaldson, Director Economic & Organisational Development**

TRIM REF **26/35844**

SUMMARY

Griffith City Council is committed to embedding privacy best practice into all business practices and decision making. Whilst the main objective of Council's Privacy Management Policy and Privacy Management Plan is to enshrine best practice in everything we do, these documents also aims to ensure Council's compliance with the Privacy and Personal Information Protection Act 1998 (PPIP Act) and Health Records and Information Privacy Act 2002 (HRIP Act).

Council has recently reviewed its Privacy Management Policy and Plan for endorsement to go on public exhibition and adoption.

RECOMMENDATION

- (a) Council endorse the Privacy Management Policy and draft Privacy Management Plan and place the documents on exhibition for a period of 28 days.**
- (b) Should any submissions be received, a report be provided to Council.**
- (c) Should no submissions be received, the Privacy Management Policy and draft Privacy Management Plan be considered adopted as at the end date of the public exhibition period.**

REPORT

The purpose of Council's Privacy Management Policy and Plan is to outline how Griffith City Council manages personal and health information in accordance with NSW privacy laws.

Council's Privacy Management Policy has been reviewed with no changes required. The Privacy Management Plan has been comprehensively reviewed with a view to making the document more user friendly and easier to understand. Both documents are presented for endorsement by Council to be placed on public exhibition.

Council is required to describe the measures it proposes to take to ensure that it complies with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

Every NSW public sector agency that is bound by the PPIP Act must prepare and implement a privacy management plan that explains:

- the agency's policies and practices for complying with the PPIP Act and the HRIP Act
- how the agency will make its staff aware of these policies and practices
- the agency's procedures for dealing with privacy internal reviews

- other relevant matters relating to the protection of the personal and health information that the agency holds.

Council's draft Privacy Management Plan complies with the Information Protection Principles (IPPs) in the PPIP Act and the Health Privacy Principles (HPPs) in the HRIP Act which regulate the collection, storage, use and disclosure of personal and health information. The principles also give members of the public a right to request access to their personal or health information or to ask for amendments to that information to ensure it is accurate.

The Privacy Management Plan also refers to relevant exemptions of the PPIP Act or HRIP Act, the Local Government Privacy Code of Practice, Council's responsibilities in terms of public registers, offence provisions and explains Council's strategies to minimise the risk of its employees committing an offence. The Plan further explains how Council will provide training and education for staff and members of the public.

A copy of Council's draft Privacy Management Plan was provided to the NSW Information and Privacy Commission (IPC) for review prior to presenting to Council.

The recommendations from the IPC (refer Attachment C) have been incorporated into Council's draft Privacy Management Plan attached to this report and are displayed as red text in the draft document.

A copy of the final adopted Plan will be provided to the IPC in accordance with section 33(5) of the PPIP Act.

OPTIONS

Council is required to adopt a Privacy Management Plan.

POLICY IMPLICATIONS

Privacy Management Policy and Privacy Management Plan.

FINANCIAL IMPLICATIONS AND RISK

Not applicable

COMPLIANCE / LEGAL / STATUTORY IMPLICATIONS AND RISK

Moderate Low Risk: Minor policy or regulatory breach resolved through amended practices.

ENVIRONMENTAL IMPLICATIONS AND RISK

Minor Low Risk: Minimal environmental impact handled internally.

REPUTATION / COMMUNITY IMPLICATIONS AND RISK

Failure to comply with Privacy requirements could result in reputational risks / risks to community members.

Serious Moderate Risk: Significant adverse public/staff reaction and/or significant negative publicity. Director intervention required over one to two weeks. Limited impact on staff morale.

SERVICE DELIVERY IMPLICATIONS AND RISK

Minor Low Risk: Nil impact to service delivery.

WHS / HR IMPLICATIONS AND RISK

Minor Low Risk: No injuries/Nil impact to service delivery.

LINK TO STRATEGIC PLAN

This item links to Council's Strategic Plan item 3.1 Undertake Council activities within a clear framework of risk management, strategic planning, policies, procedures and service standards to enhance accountability, resilience and informed decision making.

CONSULTATION

Senior Management Team

Information Privacy Commissioner

ATTACHMENTS

- (a) Privacy Management Policy - Public Policy (under separate cover)
- (b) Draft Privacy Management Plan (under separate cover)
- (c) IPC Review (under separate cover)



Privacy Management Policy GOV-CP-602 (PUBLIC POLICY)

1 Policy History

Revision No.	Council Meeting Date	Minute No.	Adoption Date
1	08/07/2003	732	08/07/2003
2	11/05/2010	0142	11/05/2010
3	09/06/2015	15/161	09/06/2015
4	24/09/2019	19/302	25/10/2019
5	25/10/2022	22/282	24/11/2022

2 Policy Objective

This Privacy Management Policy has been prepared in accordance with the requirements of the Privacy and Personal Information Protection Act 1998 (PPIP Act) and the Health Records and Information Privacy Act 2002 (HRIP Act).

This Policy aims to ensure Griffith City Council properly manages the personal and health information it collects, stores, accesses, uses and discloses in the course of its business activities.

3 Policy Statement

Council respects the privacy of its residents, customers and employees and has prepared its Privacy Management Policy in accordance with the relevant legislation and accompanying regulations.

The collection of personal and health information from individuals is required in order for Griffith City Council to perform its statutory functions and to allow the effective provision of services. It is important that the use of this information is confined to the purpose for which it was acquired.

The PPIP Act requires Council to prepare and implement a **Privacy Management Plan**. Council's Privacy Management Plan outlines how Council complies with the legislative requirements of the PPIP Act, the HRIP Act and the Privacy Code of Practice for Local Government and outlines how personal information is to be managed.

In order to properly manage the personal information it holds, it is essential for the provisions of this Policy and Council's Privacy Management Plan to be observed by all Council officials.

4 Definitions

Personal information as defined under Section 4 PPIP Act – is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This information can be on a database and does not necessarily have to be recorded in a material form. Examples of personal



information include a persons' name, address, information about family life, sexual preferences, financial information or a photograph. Personal information does not include information about an individual that is contained in a publicly available publication. Personal information, once it is contained in this format, ceases to be covered by the PPIP Act or the HRIP Act.

Health information as defined under Section 6 HRIP Act –is personal information that is information or an opinion about the physical or mental health or a disability (at any time) of an individual, or an individual's express wishes about the future provision of health services to him or her, or a health service provided (or to be provided) to an individual. Examples of health information include a blood test, immunisation history, psychological report or information about a medical appointment.

Council Officials includes Councillors, full-time, part-time and casual staff members whether they are permanent or temporary employees, consultants, volunteers, contractors and external members of Council Committees.

5 Exceptions

Nil

6 Legislation

Privacy & Personal Information Protection Act 1998 (PPIPA)
Government Information (Public Access) Act 2009 (GIPAA)
Health Records Information and Privacy Act 2002 (HRIPA)

7 Related Documents

Council's Privacy Management Plan
Council's Agency Information Guide

8 Directorate

Economic & Organisational Development

Griffith City Council



Privacy Management Plan 2026 – 2028



Contents

1. INTRODUCTION	2
1.1 What is personal information?	2
1.2 What is not personal information?	3
1.3 What is health information?	3
1.4 Why does Council collect personal and health information?	3
1.5 How does Council collect personal and health information?	4
1.6 Unsolicited information	4
1.7 Privacy Protection Notice	5
1.8 Personal and health information held by Council	5
1.9 How does Council manage personal and health information collected and held by Council?	7
1.10 How to access and amend personal and health information?	11
1.11 Promoting privacy	11
2. PUBLIC REGISTERS	12
2.1 What is a Public Register?	12
2.2 Suppression of personal information	13
3. DATA BREACHES	13
3.1 What is a data breach?	13
3.2 How will Council manage a data breach?	13
4. REVIEW RIGHTS AND COMPLAINTS PROCESS	14
4.1 Internal review	14
4.2 Internal review process	14
4.3 The role of the Privacy Commissioner in the review process	15
4.4 External review by the NSW Civil and Administrative Tribunal (NCAT)	15
5. LEGISLATIVE REQUIREMENTS	16
5.1 How Council complies with the principles	16
5.2 Exemptions	20
5.2.1 Privacy Code of Practice for Local Government	21
5.2.2 Health Records and Information Privacy Code of Practice 2005	21
5.2.3 Public Interest Directions	22
6. CONTACT DETAILS	22
7. APPROVAL AND REVIEW OF THIS PLAN	23

1. INTRODUCTION

Griffith City Council collects, stores, and uses a broad range of information for the purpose of facilitating its business. A significant part of that information is personal and health information. It is important that the community and Council officials understand how Council manages personal information.

This Privacy Management Plan has been created in accordance with Section 33 of the *Privacy and Personal Information Protection Act 1998* (NSW) to explain how personal information is collected, its purpose and how Council protects the privacy of individuals.

This Plan outlines how Griffith City Council complies with the legislative requirements of:

- [Privacy and Personal Information Protection Act 1998](#) (NSW) (PIPP Act)
- [Health Records and Information Privacy Act 2002](#) (HRIP Act)
- [Privacy Code of Practice for Local Government](#) (the Code).

Nothing in this plan is to:

- Affect any matter of interpretation of the Codes, Information Protection Principles and/or Health Privacy Principles as they apply to the Council,
- Affect any obligation at law cast upon the Council by way of representation or holding out in any manner whatsoever,
- Create, extend or lessen any obligation at law which the Council may have.

1.1 What is personal information?

Under the *Privacy and Personal Information Protection Act 1998* personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Information that can be classed as personal cannot be listed exhaustively. Below are common examples of information that generally falls into the category of personal information for the purposes of the *Government Information (Public Access) Act 2009*:

- A person's name
- Personal address and contact details – such as email address and phone numbers
- Information about a person's family life
- Financial information – including bank accounts and investments
- Employment information – including details of salaries, personnel records, recruitment information such as job recommendation and referee reports
- A person's signature
- Photographs, audio or video recordings including CCTV footage which identifies individuals
- Information about a person's hobbies or interests
- Information about a person's education – including the degree they obtained and the marks they were awarded
- Membership of voluntary or professional bodies – including trade unions
- Information about a person's religion
- Information about sexual preference
- Medical and health information.

1.2 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.

The *Privacy and Personal Information Protection Regulation 2019* 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 NSW State Archives and Records
- Public archives (within the meaning of the *Copyright Act 1968* (Cth)).

Other information that is not considered personal information can be found in [Privacy and Personal Information Protection Act 1998](#) Part 1 Section 4(3).

The following are examples of publicly available publications:

- An advertisement containing personal information in a local, city or national newspaper
- Personal information on the internet
- Books or magazines that are printed and distributed broadly to the general public
- Council Business Papers or that part that is available to the general public
- Personal information that may be a part of a public display on view to the general public.

1.3 What is health information?

Section 6 of the [Health Records and Information Privacy Act 2002](#) defines what health information is as this is a more specific type of personal information.

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

This can also include, for example, a psychological report, blood test or an x-ray, results from drug and alcohol tests, information about a person's medical appointments and personal information that is collected to provide a health service such as a name and telephone number.

1.4 Why does Council collect personal and health Information?

Council collects personal information in a variety of ways in order to efficiently perform the services and functions it delivers. Council assesses the level of personal information that is appropriate to be collected in relation to each function undertaken with a view to minimise the amount of such information that is collected and managed.

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 Council's behalf may also collect personal information. Council includes clauses in its contracts that require contractors to comply with relevant privacy obligations.

Council has a range of functions involving the collection of personal and/or health information, including:

- Levying and collecting rates
- Providing services – such as 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, licence and permits
- Providing grant funding
- Maintaining the non-residential register of electoral information
- Employment practices, including assessing fitness for work.

1.5 How does Council collect personal and health information?

Council collects personal and health information in a variety of ways including:

- Incident reports
- Medical assessment reports
- Submissions
- Application forms
- CCTV Footage
- Financial transaction records
- Contracts
- Public registers
- Customer enquiries and correspondence
- Web services and smart devices.

1.6 Unsolicited information

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

Personal information contained in petitions received in response to a call for submissions or unsolicited petitions tabled at Council meetings is managed in accordance with the *Privacy and Personal Information Protection Act 1998* (NSW).

Personal or health information disclosed publicly and recorded for the purposes of webcasting at Council Meetings is not deemed to have been collected by Council. Retention and Use principles of this information will apply to such information in Council's possession, however, Disclosure principles will not apply as the information was voluntarily disclosed with the prior knowledge that it would be recorded, broadcast via the internet to the public and made available by the Council for public viewing.

1.7 Privacy Protection Notice

Under section 10 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act), when Council collects personal information from an individual, such as their name, address, telephone number or email address, Council 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.

Where possible, individuals providing personal information will be given the opportunity to consent to the terms of the provision of the information via a Privacy Protection Notice.

Council staff are encouraged to consult with the Governance Team to ensure that each collection of personal information, and any accompanying Privacy Protection Notice is appropriate and complies with Council's privacy requirements.

The below Privacy Protection Notice should be included on all Council forms, letters, documents and other records (e.g. electronic, digital) that request and/or collect personal and/or health information from individuals:

Privacy Protection Notice

- *This information is being collected to (specify the purposes) for which the information is being collected e.g. provide a community program and service).*
- *This information is voluntarily required to process your request and will not be used for any other purpose without seeking your consent, or as required by law;*
- *Your information may comprise part of a public register related to this purpose;*
- *This form will be retained in Council's Records Management System and disposed of in accordance with the Local Government Disposal Authority;*
- *You can access and correct your personal information at any time by contacting Council.*
- *For further details on how the Griffith City Council manages personal information, please refer to our Privacy Management Plan*

1.8 Personal and health information held by Council

The following is a list of examples of the types of personal and health information and circumstances in which Council may collect this information in exercising Council functions:

1.8.1 Councillors

Council holds personal information concerning Councillors, such as:

- Personal contact information

- Code of Conduct matters
- Pecuniary interest returns
- Entitlements to fees, expenses and facilities
- Bank account details

1.8.2 Customers, ratepayers and residents

Council holds personal and health information in its records such as:

- Rates records
- Development applications and submissions
- Library membership and lending records
- Burial and cremation records
- Leases, Licences and Agreements
- Waste service records
- Customer requests
- Financial records
- Donation, Grant and Sponsorship applications
- Photos of vehicle registration plates
- Community service utilisation records
- Age and disability support records
- Responses to clean up notices regarding health issues
- Public Forum Addresses Declaration
- Council Meetings and Public Forum webcasts
- CCTV footage
- Health information – learn to swim and gym programs
- Submissions and information collected as part of Council's community engagement.

1.8.3 Employees, volunteers and contractors

Council holds personal and health information concerning its employees, volunteers and contractors, such as:

- Personal contact information
- Recruitment material
- Bank account details
- Public Interest Disclosures
- Leave and payroll data
- Performance management plans
- Code of Conduct matters
- Disclosure of interest returns
- Wage and salary entitlements
- Immunisation records and medical certificates
- Pre-employment medical information
- Workers' compensation claims
- Volunteers' medical information.

1.9 How does Council manage personal and health information collected and held by Council?

As outlined throughout this plan, Council collects and manages information from a multitude of sources in accordance with the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act). Council endeavours to make as much information available, to individuals whose information Council collects and holds, at the time of collection. Additional information is detailed below for services and functions that frequently collect personal and/or health or manage significant amounts of personal information or data.

1.9.1 Requests for service, enquiries and correspondence

Council receives a significant number of requests for service, general enquiries and correspondence which personal information is required to be collected to allow Council to perform these functions. These requests for service and enquiries are made by people:

- Over the telephone – Council does not record telephone conversations, however Council issued mobile phones do have a voicemail service
- In writing – email, letter, fax, online form
- In person – At all Council facilities such as the Administration Building, Library, Theatre, Art Gallery, Visitor's Centre, Sports Centre, Aquatic Centre, Waste facilities.

Council determines the appropriate level of personal information to be collected for each type of service request and enquiry to allow sufficient information to be an accurate record of the issue and assistance given, but Council will not collect unnecessary personal and/or health information.

If Council receives written correspondence, a full copy of whatever is sent is generally kept in Council's electronic document management system. The provision of any personal information is entirely voluntary, and in that respect personal information may be provided that is unsolicited.

Telephone conversations are not electronically recorded. If someone has an enquiry that cannot be answered straight away, the Council staff member will offer to take the person's name and telephone number or email address, so that another officer of Council can respond.

1.9.2 Complaints and regulatory functions

Council receives complaints from members of the public to investigate potential non-compliances with legislation, development consents, operating approvals etc. The majority of these investigations are handled in accordance with the relevant legislation governing Council's activities in particular functions.

Council recognises that some people may wish to remain anonymous, and clear information regarding the consequences of remaining anonymous must be provided. For example, Council may not be able to properly investigate or consider a complaint or review a matter if sufficient information about the matter is not received.

To appropriately investigate most matters, Council officers may be required to collect personal information from those parties involved, including names and address, but may also involve detailed correspondence or witness statements for complicated matters.

Council endeavours to maintain the confidentiality of complainants wherever possible, however, at times Council may be required to provide personal information of complainants to other parties due to legislative or court requirements.

1.9.3 Development assessment and land use planning

Anyone with an interest in a Development Application is welcome to make a submission, or give feedback, about a proposed development, but this must be done in writing. Any submissions made are public documents, and other people can view them upon request, Griffith City Council may redact any personal information contained in each submission.

1.9.4 Staff and recruitment

Council collects personal and/or health information from staff members as part of the recruitment process. Council will never ask for more personal information than is required for that purpose.

Staff

During the recruitment process and throughout employment, information (including personal and/or health information) is collected from staff members for various reasons, such as leave management, workplace health and safety and to help Council to operate with transparency and integrity.

Information collected by Council is retained, to the extent necessary and managed securely. In the exercise of its functions, Council collects and manages personal information about its staff including but not limited to:

- Medical conditions and illnesses
- Next of kin and contact details
- Education
- Performance and development information
- Family and care arrangements
- Secondary employment
- Conflicts of interest
- Banking details for payroll purposes
- Employment history
- Details of licences essential to the performance of an officer's role.

Recruitment

When people apply for jobs at Council, they are required to submit personal information, including their name, contact details and work history. Council provides this information to the interview panel for that particular position. The personal information is only used for the purposes of the recruitment process. After recruitment successful applicants are required to fill out various forms in order to commence employment at Council. These forms require further personal and health information, such as the applicant's:

- Bank account details
- Tax file number
- Emergency contact details
- Any disabilities that may impact their work.

These forms are sent to Human Resources to be used for employment purposes, such as payroll and setting up personnel files. This information is retained in secure storage systems.

1.9.5 Visitors and members of the public

When consultants, contractors and members of the public visit a Council facility they may be required to sign in to the premises. The record of entry may be recorded in a physical sign-in register or via a digital check in process.

Council may restrict entry or refuse provision of a service if the check in process is not observed. Any check in data collected by Council will be held securely and destroyed on a regular basis in accordance with provisions under the *State Records Act 1998* and Council's Records Management Policy.

1.9.6 Communications and stakeholder engagement

Subscriber, mailing and contact lists

Council offers residents and interested stakeholders the opportunity to stay up to date on the activities of Council via electing to subscribe to various electronic newsletters produced by Council. These services are on an opt-in basis and personal contact information is supplied to Council voluntarily by subscribers. No personal information is collected without consent and those who provide their information are advised as to how Council will manage it.

The information generally collected includes names and email addresses and in some cases areas of interest.

All lists are used solely for the purpose intended. Anyone can subscribe or unsubscribe themselves from newsletter lists or contact Council to change their details. Council does not destroy these lists; they are kept as long as they remain current. Individual entries are deleted upon request or if an error message is received in response to a Council communication.

Community engagement and public consultation

Council regularly undertakes public consultation to help guide the decision making and provision of services. Council conducts the majority of these public consultation activities via the [Connect Griffith](#) website.

Council collects information from you when you register to use the site. This may include your email address and additional demographic information as provided by you on the registration form. Council collects information about your usage of the site, such as pages visited, documents downloaded etc.

Council collects this information in order to:

- Analyse and interpret it to help meet Council's objectives and obligations
- Communicate information to you about engagement opportunities, events and other initiatives
- Respond to enquiries and otherwise engage with stakeholders.

Council website and service providers

Council engages a number of service providers who provide software, website, internet services and computer systems through which Council may collect, store or process your personal information. On occasion Council providers may have access to your personal

Page 9 of 23

information to facilitate services on behalf of Council. Council ensures that the providers adhere to the same legislative requirements in relation to Privacy.

Cookies

Council uses 'cookie' technology to collect additional website data usage and to improve its services. A cookie is a small piece of text sent to your browser by Council's website. This helps your website to remember your preferences and it makes your next visit easier and the site more useful to you. Councils uses cookies for the following purposes:

- To better understand how you interact with Council's services
- To monitor aggregate usage by users and web traffic routing on Council's services
- To improve Council's services.

Most internet browsers automatically accept cookies. You can restrict that by editing your browsers options to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit.

Personal contact details

Council engages service providers who assist Council in the distribution and communication of a variety of Council communication requirements. These may include printing and distribution of Council rate notices and/or Council newsletters etc.

To facilitate this Council's service providers are required to have access to personal information of residents and ratepayers to facilitate distribution of these materials on behalf of Council. Council ensures that the providers adhere to the same legislative requirements in relation to Privacy.

Social media

Council use social networking services such as Facebook, Instagram and LinkedIn, in addition to traditional methods, to connect with our audience. These include responding to customer enquiries in real time and promoting Council services and facilities. Council's use of social media sites also involves listening to social trends and issues that relate to Council services and events. Council use various tools to view public social media and website commentary in which Council's accounts may not necessarily be tagged. This allows Council to engage directly with members of the public to provide information and/or a better level of customer service. In doing so, Council may temporarily collect and store personal information.

To protect privacy and the privacy of others, please do not include any personal information including phone numbers and email addresses. Please do not share personal information about others. Any personal information collect by Council will be handled in line with this Plan. The social networking service will also handle your personal information for its own purposes. These sites have their own privacy policies.

Use of data from connected devices

Devices that connect to and interact with online data systems collect share, and use data to deliver convenience, efficiency and valuable insights across many areas of daily life. For Council, these technologies offer significant benefits and the potential to create strong public value. However, the large volumes of data involved may sometimes include personal, health, or otherwise sensitive information.

Because many smart devices operate passively, individuals may not always be aware when their personal information is being collected. Council will communicate what data is collected, how it is used, and who it may be shared with through centralised channels, such as the Council website, as new smart technologies are implemented.

Council will not use personal information without consent and will prioritise the use of aggregated and de-identified data wherever possible.

1.10 How to access and amend personal and health information?

Council ensures that people can access and amend information that Council holds about them.

Individuals wanting to access Council's records to confirm or amend their own personal or health information, such as updating contact details can do so by contacting Council in writing. Council will take steps to verify the identity of the person requesting access to information.

Individuals wanting to amend their own personal or health information must put the request to Council in writing:

- Email to admin@griffith.nsw.gov.au; or
- Mail to The General Manager PO Box 485 Griffith NSW 2680.

This application must contain the following information:

- The full name, date of birth and contact details of the person making the request
- State whether the application is under the PIPP Act or HRIP Act
- Explain what personal or health information the person wishes to amend
- Confirmation of the applicant's identity.

Accessing or amending other people's personal or health information

Council is restricted from giving individuals access to someone else's personal or health information unless that person provides Council with written consent. An authorised person must confirm their identification to act on behalf of someone else.

There may be other reasons Council is authorised to disclose personal and 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.

1.11 Promoting privacy

1.11.1 Compliance strategy

During induction, and on a regular basis, all employees will be made aware of this Privacy Management Plan and it will be made available on Council's Intranet and Council's website.

Council officials will be regularly acquainted with the general provisions of the:

- *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act)
- *Health Records and Information Privacy Act 2002* (HRIP Act)
- Griffith City Council's Privacy Management Plan
- Information Protection Principles
- Health Privacy Principles

- Privacy Code of Practice for Local Government
- Any other applicable Code of Practice.

1.11.2 Communication strategy

Council will promote awareness of this plan and rights under *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act), *Health Records and Information Privacy Act 2002* (HRIP Act) and this Privacy Management Plan to Council officials by:

- Providing an overview at inductions and including a copy of the plan in induction packs
- Publishing the plan on Council's internal and external websites
- Providing specialised on the job training to key groups.

1.11.3 Promoting the Plan to the community

Council promotes public awareness of this Privacy Management Plan to the community by:

- Making it publicly available and publishing it on Council's website
- Telling people about the Privacy Management Plan when they enquire about personal and/or health information
- Including privacy statements on application forms.

2. PUBLIC REGISTERS

2.1 What is a Public Register?

Under the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP 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 Council's website.

Part 6 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act) prevents Council 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.

Members of the public may enquire only in accordance with the primary purpose of any of the public registers.

Council's public registers include:

- Council Land register
- Contracts with the private sector valued from \$150,000
- Register of investments
- Register of disclosures of interest
- Register of development applications and approvals
- Register of complying development applications
- Records of approvals under Chapter 7 Part 1 of the Local Government Act 1993
- Records of impounding.

2.2 Suppression of personal information

Under section 58 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act), a person whose personal information is contained, or proposed to be contained, in a public register, may request Council to have the information removed from, or not placed on the register.

If Council is satisfied that the safety and/or wellbeing of any person would be affected by not suppressing the personal information, Council will suppress the information in accordance with the request.

An application for suppression must be made in writing, addressed to the General Manager, contain sufficient detail outlining the reasons for the request, any supporting documentation to allow for the proper assessment of the application, and be verified by a statutory declaration.

3. DATA BREACHES

3.1 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 Council's physical or electronic information or data, such as:

- Accidental loss or theft of information or equipment on which such information is stored
- Unauthorised use, access to or modification of data or information systems to gain access or make changes to data or information
- Accidental or unauthorised disclosure of personal information – such as email containing personal information sent to incorrect recipient
- Personal information published or posted on Council's website without consent
- Access to data by an authorised user for unauthorised reasons – such as an employee looking up information in a system for personal reasons in breach of the Code of Conduct
- Accidental disclosure of personal information through phishing
- Malware infection
- Disruption to or denial of IT services.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of personal information.

3.2 How will Council manage a data breach?

Council will manage an actual or suspected data breach in line with the *Privacy and Personal Information Protection Act 1998*, Mandatory Notification of Data Breach (MNDB) Scheme and Council's Data Breach Policy which is publicly available on Council's website.

The Data Breach Policy sets out how Council will respond to a data breach of Council held information.

The objectives of the policy are to:

- Provide guidance to Griffith City Council employees in responding to a data breach of council held information.
- Provide examples of situations considered to constitute a data breach.
- Detail the steps to respond to a data breach.
- Outline the considerations around notifying persons whose privacy may be affected by the breach.

The MNDB Scheme will require Council to satisfy other data management requirements, including to maintain an internal data breach incident register and maintain a public notification register.

4. REVIEW RIGHTS AND COMPLAINTS PROCESS

Griffith City Council encourages individuals to try to resolve privacy issues through an informal resolution, before undertaking the review process. Any person who may have a privacy concern can contact Council for advice.

4.1 Internal review

Under Part 5 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act) individuals have the right to seek an internal review if they believe that Council has breached the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act) or *Health Records and Information Privacy Act 2002* (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 an authorised representative of the other person.

4.2 Internal review process

Applications for an internal review must:

- Be in writing
- Specify a postal and/or email address in Australia to which the review response can be sent
- Be made within 6 months of when the affected person first became aware of the conduct or decision that is the subject of the application.

The Privacy Officer or their delegate will conduct the internal review. If the internal review is about the conduct of the Privacy Officer, the General Manager will appoint another person to conduct the internal review. The reviewing officer will refer to the Privacy Commissioner's guidance materials when carrying out an internal review. [IPC - Fact Sheet & Checklist - Internal Review](#)

Council will acknowledge receipt of an internal review within 5 working days and complete an internal review within 60 calendar days.

Within 14 days of completing an internal review, Council will notify the applicant of the following:

Page 14 of 23

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

The contact details for Council's Privacy Officer are:

Council's Privacy Contact Officer

Leanne Austin

Governance Manager

Telephone: 1300 176 077

Email: admin@griffith.nsw.gov.au

Alternatively, you can download a generic form [here](#) to submit to Council.

4.3 The role of the Privacy Commissioner in the review process

The Privacy Commissioner has an oversight role in how privacy complaints are handled and is entitled to make submissions to Council regarding internal reviews.

If Council receives an internal review application, it will:

- Notify the Privacy Commissioner of the application as soon as practicable
- Keep the Privacy Commissioner informed of the progress of the internal review
- Inform the Privacy Commissioner of the findings of the review and the action proposed to be taken by Council in relation to the matter.

An individual can also make a complaint directly to the Privacy Commissioner about an alleged breach of their privacy. Your complaint can be sent to ipcinfo@ipc.nsw.gov.au, or you can complain verbally by contacting the IPC on 1800 472 679.

For more information visit the Information and Privacy Commission website: [Making a privacy complaint](#).

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

If the applicant remains unsatisfied with the outcome of an internal review or is not notified of an outcome within 60 days, they have the right to seek an external review and may make application to the NSW Civil and Administration Tribunal (NCAT) for a review of Councils conduct.

An application for external review can only be made after an internal review has been completed and must be made within 28 days from the date of the internal review decision.

5. LEGISLATIVE REQUIREMENTS

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

For more information, please refer directly to the relevant legislation or contact Griffith City Council.

The *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act) provides for the protection of personal information by means of 12 Information Protection Principles whilst *Health Records and Information Privacy Act 2002* (HRIP Act) provides for the protection of health information by means of 15 Health Information Protection Principles.

Griffith City Council complies with the Information Protection Principles (IPPs) prescribed under PIPP Act and the Health Privacy Principles (HPPs) prescribed under HRIP Act as outlined below.

5.1 How Council complies with the principles

5.1.1 Collection

Lawful (Information Protection Principle 1, Health Privacy Principle 1)

- Council will only collect personal information for a lawful purpose that is directly related to a function or activity of Council and is reasonably necessary for that purpose.
- Council will not collect any more personal information than is reasonably necessary to fulfill its proper functions.
- Council will 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
- Anyone engaged by Council as a contractor or consultant that involves the collection of personal information must agree to be bound not to collect personal information by any unlawful means.

Direct (Information Protection Principle 2, Health Privacy Principle 3)

- Council will only collect information directly from the individual to whom the information relates (or parents/guardians if the individual is under the age of 16), unless authorised by the individual to whom the information relates.
- The Code makes provision for Council to depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.

- Council may collect personal information from other public sector agencies in respect of specific statutory obligations where it is authorised or required not to comply with the principle under any Act or Law.

Open (Information Protection Principle 3, Health Privacy Principle 4)

- Council will take reasonable steps to inform people why their information is being collected, what it will be used for, and to whom it will be disclosed.
- A Privacy Statement is included on Council's website and on forms where personal information is collected.

Relevant (Information Protection Principle 4, Health Privacy Principle 2)

- Council will take reasonable steps to ensure that personal or health information collected is relevant and accurate, is not excessive and does not unreasonably intrude into people's personal affairs.
- Council will, in normal circumstances, rely on the provider of the information regarding accuracy and completeness, although in special circumstances some verification processes may be necessary or appropriate.

5.1.2 Storage

Secure (Information Protection Principle 5, Health Privacy Principle 5)

- Council will store personal information securely, keep it no longer than necessary and dispose of it appropriately. This information will also be protected from unauthorised access, use, modification or disclosure.
- Council ensures personal information is securely stored in accordance with IPP 5 by implementing appropriate physical and administrative safeguards. Access is restricted to authorised personnel, systems are protected through security controls and records are securely retained and disposed of in line with records management requirements
- Council securely stores health information using appropriate physical and administrative safeguards, including restricted access, secure systems and staff confidentiality requirements. Health information is only accessible to authorised personnel and is protected throughout its lifecycle, including secure disposal when no longer required.
- Council's Records and Information Management Policy provides further guidance regarding management of Council records.

5.1.3 Access and accuracy

Transparent (Information Protection Principle 6, Health Privacy Principle 6)

- Council is transparent about the information that is held and why it is used.
- Individuals can request to access their own information to determine whether Council hold their information, the nature and main purposes for which it is held, how it is stored and how long it will be held for.

- Should an individual seek information generally about the nature of any information held, council may ask for advice on the types of dealings the applicant has had with council to assist to conduct the search.

Accessible (Information Protection Principle 7, Health Privacy Principle 7)

- Council will allow people access to their information on receipt of a written request without unreasonable delay or expense.
- Compliance of this principle does not allow disclosure of information about other people. Where an individual's personal and/or health information is contained in documents that also contain information about others, any application for access will need to be made and processed under the Government Information (Public Access) Act 2009.

Correct (Information Protection Principle 8, Health Privacy Principle 8)

- Council will allow people to update, correct or amend their information, if necessary, to ensure information is accurate, relevant, up to date, complete and not misleading.
- Changes of name, address and other minor amendments, require appropriate supporting documentation. Where substantive amendments are involved, a written application will be required. The application should set out the grounds on which changes are sought.
- Council will seek to notify recipients of amendments to personal information as soon as possible, where it is reasonably practicable.

5.1.4 Use

Accurate (Information Protection Principle 9, Health Privacy Principle 9)

- Council will take all reasonable steps necessary to make sure the personal information is relevant, accurate, up to date and complete before using it.
- This includes verifying information at the point of collection, enabling individuals to update their details, implementing system controls and requiring staff to confirm accuracy prior to use.
- Council takes reasonable steps to ensure health information is accurate, up to date, complete and relevant before use. This includes verifying information with individuals and requiring staff to maintain accurate records.

Limited (Information Protection Principle 10, Health Privacy Principle 10)

- Council will only use personal information for the purpose it was collected, unless the person has consented to another use or:
 - The other purpose is directly related to the purpose for which the information was collected.
 - The use is necessary to prevent or lessen a serious and imminent threat to the

- life or health of any person.
- The use is reasonably necessary for law enforcement purposes or protection of public revenue.
- The information is to be used for a reason as specified under 'Exemptions, directions and codes of practice' section of this plan.
- Council may use information for a variety of purposes. For example, the names and addresses of individual property owners kept as part of Councils rates record to:
 - Notify neighbours of proposed development
 - Evaluate a road opening or obstruction
 - Evaluate tree preservation orders

5.1.5 Disclosure

Restricted / Limited (Information Protection Principle 11, Health Privacy Principle 11)

- Council does not disclose personal information without consent, to a person (other than the individual to whom the information relates) or other body, unless:
 - The disclosure is directly related to the purpose for which the information was collected.
 - Council believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of any person.
 - The individual expressly consents to the disclosure. For example, Council may provide information about an employee or former employee to a potential employer, or verifying details concerning wages to a financial institution.
 - The disclosure is made in connection with proceedings for an offence, law enforcement purposes, the protection of public revenue or to investigate an offence where there are reasonable grounds to believe an offence may have been committed.

Safeguarded (Information Protection Principle 12)

- Council does not disclose sensitive personal information without consent unless it is necessary to prevent a serious and imminent threat to the life or health of an individual, in relation to the following:
 - Ethnicity or racial origin
 - Political opinions
 - Religious or philosophical beliefs
 - Health or sexual activities
 - Trade union membership.
- Council will not disclose this information to any person or body that is outside of NSW unless:
 - The recipient of the information is subject to similar information privacy principles or laws regarding personal information, or
 - It is necessary to investigate an offence or where there are reasonable grounds to believe an offence has been or may be committed.
 - The consent of the person cannot reasonably be obtained and the disclosure is made by an authorised person to another authorised person. Authorised person means – a medical practitioner, health worker, or other official providing health or community services who is employed or engaged by a public sector agency.

Page 19 of 23

- Where a disclosure is to be made to a public sector agency for the purpose of informing the Minister for Local government or the Premier about a matter within their administration.

5.1.6 Identifiers and anonymity

Identifiers (Health Privacy Principle 12)

- Council will only give an identification number to health information if it is reasonably necessary to carry out Council functions effectively.

Anonymity (Health Privacy Principle 13)

- Where Council provides health services, it will allow for individuals to stay anonymous where it is lawful and practical to do so.

5.1.7 Transfers

Transfers (Health Privacy Principle 14)

- Council will only transfer health information outside of NSW where satisfied that this is required by law, or otherwise in accordance with the Health Records and Information Privacy Act 2002 (HRIP Act).

5.1.8 Linkage of health records

Linkages (Health Privacy Principle 15)

- Council may link health information with other agencies or organisations only where it is authorised by law and necessary for functions such as public health, safety, service coordination or emergency management. This may include collaboration with NSW Health, emergency services, community service providers and other government agencies.
- Any such linkage is subject to strict governance controls, including data minimisation, access restrictions, security safeguards, and (where applicable) de-identification and ethical approval processes.

5.2 Exemptions

Council is committed to complying with the Information Protection Principles (IPPs) under the Privacy and Personal Information Protection Act 1998 (PPIP Act) and the Health Privacy Principles (HPPs) under the Health Records and Information Privacy Act 2002 (HRIP Act).

Council recognises that, in certain circumstances, these principles may be lawfully modified or do not apply through exemptions provided under legislation, regulations, Privacy Codes of Practice, or Public Interest Directions.

Council ensures that any reliance on an exemption or modification is:

- Lawful and properly authorised
- Necessary for Council functions

- Proportionate and limited to the specific circumstances
- Documented and subject to appropriate governance oversight.

5.2.1 Privacy Code of Practice for Local Government

Part 2, Division 3 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act) contains exemptions that may permit Griffith City Council to not comply with Information Protection Principles in certain situations. These include the following:

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

For example, Section 23(3) of the PIPP Act provides that Council 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.

Council must comply with the *Privacy Code of Practice for Local Government* as prepared by the Office of the Privacy Commissioner. Under the *Privacy Code of Practice for Local Government* where it is reasonably necessary, Council may indirectly collect and use personal information to confer an award, prize or similar form of personal recognition on the person about who the information relates.

The *Privacy Code of Practice for Local Government* also permits Council to use personal information for a purpose other than the purpose for which it was collected where the use is in pursuance of Council's lawful and proper functions and Council is satisfied that the personal information is reasonably necessary for the exercise of those functions.

For example, the Rates Record that Council holds under section 602 of the *Local Government Act 1993* may be used to:

- Notify neighbours of a proposed development
- Evaluate a road opening
- Evaluate a tree preservation order.

Under section 62-68 of the *Privacy and Personal Information Protection Act 1998 (NSW)* (PIPP Act) it is an offence for Council 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.

5.2.2 Health Records and Information Privacy Code of Practice 2005

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

The *Health Records and Information Privacy Code of Practice 2005* applies to Council. 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.

Under section 68-70 of the *Health Records and Information Privacy Act 2002* (HRIP Act) it is an offence for Council to:

- Intentionally disclose or use health information for an unauthorised purpose
- Offer to supply health information that has been disclosed unlawfully.

5.2.3 Public Interest Directions

A Public Interest Direction is issued by the NSW Privacy Commissioner and allows a temporary modification or waiver of one or more IPPs or HPPs where this is in the public interest. Health Public Interest Directions may similarly modify HPPs in specific circumstances. Examples include:

- Pilot or trial programs
- Data linkage initiatives
- Cross-agency or innovative service delivery projects

Council will:

- Identify and comply with any Public Interest Directions that apply to its activities
- Ensure conditions attached to a Public Interest Direction are strictly followed
- Limit reliance on Public Interest Directions to the approved scope and timeframe

Where Council identifies a need to depart from the privacy principles that is not otherwise authorised, it will:

- Seek advice from the Information and Privacy Commission (IPC)
- Consider applying for a Public Interest Direction where appropriate.

6. CONTACT DETAILS

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

Council's Privacy Contact Officer
Leanne Austin
Governance Manager
Telephone: 1300 176 077
Email: admin@griffith.nsw.gov.au

Griffith City Council
Telephone: 1300 176 077
Email: admin@griffith.nsw.gov.au
Street address: 1 Benerembah Street Griffith NSW 2680
Postal address: PO Box 485 Griffith NSW 2680
[Contact us | GCC](#)

Information and Privacy Commission NSW
Email: ipcinfo@ipc.nsw.gov.au
Telephone: 1800 472 679
Street address: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000
Postal address: GPO Box 7011, Sydney NSW 2001
Interpreter Service: 131 450
National Relay Service: 133 677 (If you are deaf or have a hearing or speech impairment)
[Contact us](#)

NSW Civil and Administrative Tribunal
Telephone: 1300 006 228
Interpreter Service: 13 14 50
National Relay Service: 1300 555 727
Email: aeod@ncat.nsw.gov.au
Street address: Level 10 John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000
Postal address: PO Box K1026, Haymarket NSW 1240
[Contact us | NSW Civil and Administrative Tribunal](#)

7. APPROVAL AND REVIEW OF THIS PLAN

Council approved this plan on xxxxx.

This Plan is to be reviewed in 2028.



Enquiries: Stephanie Li

Telephone: 1800 472 679

Our reference: IPC26/AU000022

16 June 2026

Ms Leanne Austin
Governance Manager
Griffith City Council
By email to: Leanne.Austin@griffith.nsw.gov.au

Dear Ms Austin

Review of Draft Revised Privacy Management Plan for Griffith City Council

I refer to the draft revised Privacy Management Plan (**PMP**) for Griffith City Council (**the Agency**) which was received by the Information & Privacy Commission (**IPC**) on 30 March 2026

A PMP is an integral part of a public sector agency's corporate governance. It will assist in guiding not only that agency's operations but also its compliance monitoring regime.

The IPC's role includes promoting privacy as well as preparing reports recommending legislative, administrative, or other actions in the interests of privacy. The IPC provides independent reports on the functioning of the privacy legislation to the NSW Parliament.

The IPC assists public sector agencies in preparing and implementing PMP's. To assist you with your draft revised PMP, a copy of the PMP checklist is **enclosed**. This was developed for public sector agencies, so as to enable our feedback to be delivered in a systematic way.

The IPC has reviewed the Agency's draft revised PMP and attached is our recommended amendments for your consideration. If the amendments are adopted, it would be appreciated if you could please forward a copy of the amended PMP to the IPC as soon as practicable.

I would appreciate any feedback you may have regarding the implementation of the Agency's draft revised PMP or any other privacy-related matters for the Agency.

Should you or any officer of the Agency have any enquiries about this correspondence, please do not hesitate to contact the IPC on 1800 472 679, or by email at ipcinfo@ipc.nsw.gov.au and quoting our reference for this matter: IPC26/AU000022.

Yours sincerely


Stephanie Li

Senior Regulatory Officer

Enclosed: IPC PMP Checklist for IPC26/AU000022.



information
and privacy
commission
new south wales

Privacy Management Plans

June 2026

Who is this information for?	NSW public sector agency staff seeking support on Privacy Management Plans
Why is this information important to them?	This checklist can be used by public sector staff to assess the content of their agency's Privacy Management Plan once it has already been prepared.

Section 33 of the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) requires agencies to have a privacy management plan (**plan**). A plan sets out an agency's commitment to respecting the privacy rights of clients, employees, and members of the public. It should also explain an agency's practices and procedures in handling personal information under the PPIP Act and health information under the *Health Records and Information Privacy Act 2002* (**HRIP Act**).

This checklist does not prescribe the structure and format a plan should follow. Rather, it is a useful tool for an agency to assess the content of its plan once it has already been prepared.

The NSW Privacy Commissioner also uses this checklist to assess the quality of plans they receive from agencies.

For practical information on how to write a plan, please refer to the [Guide to Making Privacy Management Plans](#).

Review Questions

	Yes	Part	No	Comments
General				
1. Does the plan mention the agency's requirement to have a plan?	☒	☐	☐	
2. Does the plan describe the main kinds of personal and health information managed by the agency? <i>Tip: Think about this question in context of the functions and activities of the agency</i>	☒	☐	☐	The PMP includes numerous examples of the kinds of personal and health information it holds.
Information Protection Principles (sections 8 -19, Part 1, Division 1 of the PPIP Act)				
3. Does the plan explain how the personal information the agency collects is related to the agency's functions and activities (IPP 1)? <i>e.g. Enquiries, complaints handling, core business, human resources, recruitment</i>	☒	☐	☐	The PMP provides a list of functions and how the collection is relation to those functions.
4. Does the plan indicate when the agency collects personal information from the person and when it is collected from third parties (IPP 2)?	☒	☐	☐	
5. Does the plan explain how and when a person is notified that their personal information is being collected (IPP 3)?	☒	☐	☐	
6. Does the plan explain how the agency ensures that the collection of personal information is relevant, not excessive and is not an unreasonable intrusion (IPP 4)?	☒	☐	☐	The PMP may benefit from the Agency explaining how it will ensure collection of personal information is not excessive.

Privacy Management Plans

Checklist

	Yes	Part	No	Comments
7. Does the plan generally explain how the agency stores, protects and disposes of personal information (IPP 5)?	☐	☒	☐	The PMP includes a description of IPP 5 but will benefit from more details about how it complies with IPP 5. A reference to any policies or procedures the Agency has in place to ensure compliance sufficient security and storage of personal information may be useful.
8. Does the plan explain how the agency helps a person find out: <ul style="list-style-type: none"> whether the agency holds their personal information the nature of the information the main purpose for which it is collected their right of access (IPP 6)? 	☒	☐	☐	
9. Does the plan set out how a person can access their personal information (IPP 7)?	☒	☐	☐	
10. Does the plan set out how a person can request an amendment to their personal information (IPP 8)?	☒	☐	☐	The PMP provides good detail about how an individual can request to amend their personal information, along with relevant contact information to make a request.
11. Does the plan explain how the agency checks the accuracy of personal information before using it (IPP 9)?	☐	☒	☐	The PMP includes a description of IPP 9 but will benefit from more details about how it complies with IPP 9.
12. Does the plan mention how the agency limits its use of personal information (IPP 10)?	☒	☐	☐	
13. Does the plan mention how the agency limits disclosure of personal information (including other jurisdictions) (IPP 11)?	☒	☐	☐	
14. Does the plan explain how the agency deals with sensitive personal information (IPP 12)?	☒	☐	☐	
Health Privacy Principles (clauses 1-15, Schedule 1 to the HRIP Act)				
15. Does the plan explain how the health information the agency collects is related to the agency's functions and activities (HPP 1)? <i>e.g. Enquiries, complaints handling, core business, human resources, recruitment</i>	☒	☐	☐	
16. Does the plan explain how the agency ensures that the collection of personal information is relevant, not excessive and is not an unreasonable intrusion (HPP 2)?	☒	☐	☐	The PMP may benefit from the Agency explaining how it will ensure collection of health information is not excessive.
17. Does the plan indicate when the agency collects health information from the person and when it is collected from third parties (HPP 3)?	☒	☐	☐	
18. Does the plan explain how and when a person is notified that their health information is being collected (HPP 4)?	☒	☐	☐	
19. Does the plan explain how the agency stores, protects and disposes of health information (HPP 5)?	☐	☒	☐	The PMP includes a description of HPP 5 but will benefit from more details about how it complies with HPP 5. A reference to any policies or procedures the

Privacy Management Plans

Checklist

	Yes	Part	No	Comments
				Agency has in place to ensure compliance sufficient security and storage of health information may be useful.
20. Does the plan explain how the agency helps a person find out: <ul style="list-style-type: none"> whether the agency holds their health information the nature of the information the main purpose for which it is collected their right of access (HPP 6)? 	☒	☐	☐	
21. Does the plan set out how a person can access their health information (HPP 7)?	☒	☐	☐	
22. Does the plan set out how a person can request an amendment to their health information (HPP 8)?	☒	☐	☐	
23. Does the plan mention how the agency checks the accuracy of health information before using it (HPP 9)?	☐	☒	☐	The PMP includes a description of HPP 9 but will benefit from more details about how it complies with HPP 9.
24. Does the plan mention how the agency limits its use of health information (HPP 10)?	☒	☐	☐	
25. Does the plan mention how the agency limits disclosure of health information (HPP 11)?	☒	☐	☐	
26. Does the plan mention whether the agency assigns identifiers to individuals (if applicable) (HPP 12)?	☒	☐	☐	The PMP may benefit from a brief explanation and example of circumstances which would require the Agency to assign identifiers to individuals.
27. Does the plan mention whether it gives individuals the opportunity to remain anonymous (HPP 13)?	☒	☐	☐	
28. Does the plan mention whether the agency discloses health information to individuals or bodies outside of NSW (HPP 14)? <i>e.g. Commonwealth, interstate, overseas</i>	☒	☐	☐	
29. Does the plan mention whether the agency includes health information in a health records linkage system (if applicable) (HPP 15)?	☐	☐	☒	The PMP does not mention HPP 15 and will benefit from the addition of a new section about HPP 15.
30. Does the plan mention whether any exemptions in the PPIP Act or the HRIP Act are particularly relevant to the agency?	☒	☐	☐	
Exemptions				
31. Does the plan mention whether there are any codes of practice or public interest directions relevant to the agency?	☐	☒	☐	The PMP refers to codes of practice but does not refer to relevant public interest directions. The Agency may wish to consider whether there are any relevant public interest directions and provide more details within the PMP.
32. Does the plan mention whether there is any relevant legislation that allows the agency not to comply with any of the IPPs or HPPs?	☒	☐	☐	

Privacy Management Plans

Checklist

	Yes	Part	No	Comments
33. Does the plan mention whether the agency has any Memorandums of Understanding or referral arrangements with other agencies?	☐	☐	☒	The Agency may wish to consider whether this applies and provide more details within the PMP if this is relevant.
34. If any of 31 to 33 are applicable, does the plan briefly explain how they actually impact the agency's handling of personal or health information?	☒	☐	☐	
Public registers				
35. Does the plan advise whether the agency has any public registers that contain personal or health information?	☒	☐	☐	
36. If so, does the plan explain whether the personal or health information in these public registers can be accessed, and how?	☒	☐	☐	The PMP explains the type of information that may be included in the public registers and that enquiries can be made via the Agency's website.
37. Does the plan explain how a person can apply for personal or health information to be suppressed in a public register?	☒	☐	☐	The PMP may benefit from the Agency providing further information about the criteria for suppressions and the relevant Agency contact information to make a submission.
Internal reviews and complaints				
38. Does the plan explain a person's right to seek an internal review?	☒	☐	☐	
39. Does the plan set out the internal review process? <i>e.g. How to apply for one, relevant timeframes, who makes the decision, how decisions are made, how the applicant is advised of the decision.</i> Tip: If an agency does not have its own form, it can use the generic form on our website.	☒	☐	☐	
40. Does the plan explain the notification process and the role of the Privacy Commissioner?	☒	☐	☐	
41. Does the plan explain a person's right to an external review from the NSW Civil and Administrative Tribunal (NCAT) if dissatisfied with the internal review outcome?	☒	☐	☐	
42. Does the plan set out the agency's alternative complaint process at the agency if a person wants to resolve an issue informally?	☐	☒	☐	The PMP mentions that the Agency encourages individuals to resolve privacy issues through an informal resolution and to contact Council for advice. The PMP will benefit from providing more details about such process.
43. Does the plan include the option to make a complaint to the Privacy Commissioner?	☐	☒	☐	The PMP may benefit from the inclusion of further information about this process along with any relevant links. The Agency may wish to visit the IPC's website for more detail – here .
Mandatory Notification Data Breach (MNDB)				

Privacy Management Plans

Checklist

	Yes	Part	No	Comments
44. Does the plan provide information on how data breaches will be managed by the agency?	☒	☐	☐	
45. Does the plan provide information on how to access the agency's Data Breach Policy and provide a link to the Policy?	☐	☐	☒	The PMP will benefit from including a link to access the policy.
46. Does the plan provide information on the process for assessing and notifying eligible data breaches to the Privacy Commissioner?	☐	☒	☐	Whilst the PMP explains the meaning of a data breach and refers to the Data Breach Policy, it will benefit from including a summary about the process for informative purposes.
Offences				
47. Does the plan generally explain the offences in the PPIP Act and HRIP Act?	☒	☐	☐	
Raising awareness of the plan and using it				
48. Does the plan set out how the agency trains staff to use the plan and comply with their privacy obligations? <i>e.g. Induction, periodic training, day-to-day work, what staff should do if unsure about a privacy issue</i>	☒	☐	☐	The PMP mentions that during induction and on a regular basis all employees are made aware of the PMP and the relevant privacy laws and Codes.
49. Does the plan set out how the agency educates members of the public in the agency's privacy obligations and their privacy rights? <i>e.g. Published on the web, mentioned on forms that collect personal or health information</i>	☐	☒	☐	The Agency explains its communication strategy. The PMP may be improved by including the links to the Agency's website and relevant guidance or promotion material.
Other agencies				
50. Does the plan cover more than one agency?	☐	☐	☒	
51. If so, are the agencies listed individually?	☐	☐	☐	N/A
52. Does the plan go into enough detail about the functions and the personal and health information managed by each agency covered?	☐	☐	☐	N/A
Privacy-related policies and procedures				
53. Does the plan describe how the agency devises its policies and practices to comply with the PPIP Act and the HRIP Act?	☐	☐	☒	The PMP will benefit from more details about how it devises its policies and practices.
54. Does the plan specify whether there are other policies and procedures relevant to the plan?	☒	☐	☐	The Agency mentions the Data Breach Policy, Records Management Policy and Privacy Code of Practice for Local Government.
55. If so, does the plan mention how the agency makes these documents available to staff and members of the public? <i>Tip: Website links can be useful here</i>	☐	☒	☐	The PMP includes a link to the Privacy Code of Practice for Local Government but will also benefit from providing the links to all other relevant material.
Accuracy				
56. Is there an adoption/version date on the plan?	☒	☐	☐	This plan is for 2026 to 2028.
57. Is there a review date on the plan?	☒	☐	☐	The review date is 2028.

Privacy Management Plans

Checklist

	Yes	Part	No	Comments
58. Are any references to legislation in the plan current?	☒	☐	☐	
59. If applicable, do the website links in the plan work?	☒	☐	☐	
Readability				
60. Is the structure of the plan logical?	☒	☐	☐	
61. Does the plan have a table of contents?	☒	☐	☐	
62. Is the level of detail and length of the plan appropriate?	☒	☐	☐	
63. Is the plan written in plain English? <i>Tip: Show your draft plan to a new staff member or a member of the public and ask whether they can understand it</i>	☒	☐	☐	
64. Is the plan helpful to members of the public and staff?	☒	☐	☐	
Contact details				
65. Does the plan include current contact details for the Privacy Contact Officer or relevant privacy section at the agency for privacy-related enquiries?	☒	☐	☐	
66. Does the plan include current contact details for the Information and Privacy Commission NSW (IPC)?	☒	☐	☐	
67. Does the plan include current contact details for the NSW Civil and Administrative Tribunal (NCAT)?	☒	☐	☐	
Accessibility				
68. Does the plan explain how the agency makes it available to staff and members of the public? <i>e.g. Website, over the counter, mailed out on request</i>	☒	☐	☐	
69. Will the plan be on the agency's website and easy to find? <i>Note: The plan is a policy document (open access information) under the Government Information (Public Access) Act 2009 (GIPA Act)</i>	☒	☐	☐	
Automated Decision Making (ADM)				
70. Does the plan include a description of the types of ADM systems used, and their purpose? <i>Note: ADM refers to a fully or partially automated technical system, used in decision-making, which may or may not involve the use of AI, and affects people.</i>	☐	☐	☒	The PMP makes no reference to ADM and the Agency may wish to consider incorporating a section to explain ADM, its potential use and disclosure. Please refer to questions 70 to 76 which provide details to be included in the PMP. Additional feedback provided in the "general comments" below.
71. Does the plan include information about the kinds of personal information used in ADM systems?	☐	☐	☒	
72. Does the plan describe the types of decisions made by ADM using personal information?				

Privacy Management Plans

Checklist

	Yes	Part	No	Comments
73. Does the plan explain who personal information may be shared with?				
74. Does the plan describe the ways in which its use of ADM affects members of the public?				
75. Does the plan include a process for how individuals can request more information?				
76. Does the plan include information about how an individual can challenge or appeal a decision made by, or with the assistance of, ADM?				
Artificial Intelligence (AI)				
77. Does the plan include a description of the types of AI systems used, and their purpose? <i>Note: AI refers to 'the ability of a computer system to perform tasks that would normally require human intelligence, such as learning, reasoning, and making decisions'. AI encompasses various specialised domains that focus on different tasks.</i>	☐	☐	☒	<p>The PMP makes no reference to AI and the Agency may wish to consider incorporating a section to explain AI, its potential use and disclosure. Please refer to questions 77 to 85 which provide details to be included in the PMP.</p> <p>Additional feedback provided in the "general comments" below.</p>
78. Does the plan include information about the kinds of personal information used in AI systems?				
79. Does the plan describe the way its use of personal information in AI affects members of the public?	☐	☐	☐	
80. Does the plan include a process for how individuals can request more information about the use of AI?				
81. Does the plan include information about how an individual can challenge or appeal a decision made using AI?				
82. Does the plan explain how and whether their personal information is used to train AI?				
83. Does the plan explain how individuals may access their personal information held in AI systems?				
84. Does the plan explain how information is shared with AI platforms and providers?				
85. Does the plan explain where the information shared with AI platforms and providers is stored?				

General comments

The Agency is encouraged to:

1. provide more details about some of the IPPs and HPPs as highlighted in this letter.
2. elaborate further about its policies and codes and include all the relevant links.
3. inform the public about ADM and AI and follow the guidance provided in this letter.

The Agency should also take this opportunity to consider and review any of its technology-based platforms which may involve the use of personal information and ensure that any such technologies in so far as they relate to the collection, use, disclosure or sharing of personal information is also encompassed in the PMP. We draw the Agency's attention to the recently published report by the Privacy Commissioner (jointly with Information Commissioner) on the IPC website which outlines how PMPs should have regard for these matters should be included. The report is available [here](#).

Privacy Management Plans

Checklist

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au

NOTE: The information in this checklist is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.