Ku-ring-gai Council

Policy

Privacy Management Plan

Version Number 2

Adopted: 3 March 2023

Effective: 21 June 2023

Privacy Management Plan

Table of Contents

Controlled Document Information

Authorisation Details

This is a Controlled Document. Before using this document check it is the latest version by referring to Council's Controlled Document Register. Unless otherwise indicated, printed or downloaded versions of this document are uncontrolled.			
Controlled Document Number:	186	**TRIM Record No:**	2021/259508
Controlled Document Type:	Policy		
Controlled Document Name:	Privacy Management Plan		
Version Number:	2		
Department:	Corporate		
Distribution:	Internal and External		
Review Period: **Max < 4 years**	4 years	**Next Review Date:**	November 2023 (to reflect changes required by the Privacy and Personal Information Protection Amendment Act 2022)
Document Status:	Approved		
Approval Type:	Adopted by Council		
Version Start Date:	21 June 2023	**Version End Date:**	TBC

Related Document Information, Standards & References

Related Legislation and Statutory Instruments:	*Children and Young Persons (Care and Protection) Act 1998* *Companion Animals Act 1998* *Copyright Act 1968 (Cth)* *Criminal Records Act 1991* *Crimes Act 1900* *Government Information (Public Access) Act 2009* *Government Information (Public Access) Regulation 2018* *Health Records and Information Privacy Act 2002* *Health Records and Information Privacy Regulation 2022* *Independent Commission Against Corruption Act 1988* *Local Government Act 1993* *Privacy Act 1988 (Cth)* *Privacy and Personal Information Protection Act 1998* *Privacy and Personal Information Protection Regulation 2019* *State Records Act 1998* *Surveillance Devices Act 2007* *Workplace Surveillance Act 2005*
Related Policies	Agency Information Guide Code of Conduct

	Complaints Management Policy Compliance Policy Computer Access Policy Covert Electronic Surveillance for Illegal Dumping Policy Cyber Incident Response Plan Information and Cyber Security Policy Overt Electronic Surveillance in Public Places Policy
Related Instruments	Privacy Code of Practice for Local Government 2019
Other References	Information and Privacy Commission NSW Civil and Administrative Tribunal

Version History

Version Number	Version Start Date	Version End Date	Author	Details and Comments
1	5 July 2000	24 June 2008	Manager Records and Governance	First version
2	25 June 2008	19 August 2008	Manager Records and Governance	Review and update
2.1	20 August 2008	2 August 2011	Manager Records and Governance	Update after revised Code of Conduct approved Min 239 CM 22 July 2008
3	3 August 2011	25 February 2013	Manager Records and Governance	Review and update
3.1	26 February 2013	4 June 2023	Manager Records and Governance	Update after revised Model Privacy Management Plan issued by DLG (Version 3.1 Record Number: 985377[v3])
4	5 June 2023	TBC	Manager Governance and Corporate Strategy	Review and update. Added the IPC's *Privacy Code of Practice for Local Government* December 2019 and added comments from IPC

Need help?

This document contains important information. If you do not understand it, please call the Translating and Interpreting Service on 131 450. Ask them to phone 9424 0000 on your behalf to contact Ku-ring-gai Council. Business hours: Monday to Friday, 8.30am-5pm.

Simplified Chinese

需要帮助吗？

本文件包含重要信息。如果您不理解本文件，请致电翻译口译服务 131 450。让其代表您致电 9424 0000 联系Ku-ring-gai议会。营业时间：周一至周五，上午8.30—下午5:00。

Traditional Chinese

需要幫助嗎？

本檔包含重要資訊。如果您不理解本檔，請致電翻譯口譯服務131 450。讓其代表您致電9424 0000聯繫Ku-ring-gai議會。營業時間：週一至週五，上午8.30—下午5:00。

Japanese

お困りですか?

この文書には、重要な情報が含まれています。ご不明な点があれば、「翻訳・通訳サービス」（電話131 450）までお電話いただき、あなたに代わって、クーリンガイ（Ku-ring-gai）議会に連絡するよう、ご依頼ください。営業時間：月曜日～金曜日（8.30am-5pm）。

Korean

도움이 필요하십니까?

이 문서에는 중요한 정보가 담겨 있습니다. 여러분이 이해할 수 없다면, TIS (번역 및 통역 서비스)의 131 450 번으로 전화하십시오. 9424 0000 번으로 여러분을 대신하여 전화해서 쿠링가이 카운슬을 연락해 달라고 요청하십시오. 영업 시간: 월요일-금요일, 오전 8시30분-오후 5시.

Hindi

सहायता चाहिए?

इस दस्तावेज़ में महत्वपूर्ण जानकारी है। यदि यह आपको समझ नहीं आती, तो कृपया अनुवाद और दुभाषिया सेवा को 131 450 पर कॉल करें, और इस सेवा को आपकी ओर से फ़ोन: 02 9424 0000 पर व्यावसायिक घंटों के दौरान, सोमवार से शुक्रवार, सुबह 8.30 से शाम 5.00 बजे तक कू-रिंग-गई काउन्सिल से संपर्क करने के लिए अनुरोध करें ।

Persian

آیا به کمک نیاز دارید؟

این مدرک حاوی اطلاعات مهمی است. اگر آنها را نمی فهمید، خواهش می کنیم به خدمات ترجمه نوشتاری و گفتاری (Translating and Interpreting Service) به شماره ۱۳۱ ۴۵۰ تلفن کنید و از آن سرویس بخواهید از جانب شما با شهرداری کورینگای (Ku-ring-gai Council) در ساعات کاری، دوشنبه تا جمعه از ساعت ۸:۳۰ صبح تا ساعت ۵:۰۰ بعد از ظهر با شماره تلفن ۰۲ ۹۴۲۴ ۰۰۰۰ تماس بگیرند.

Introduction

People reasonably expect to be able to determine how, and for what purpose their personal and health information is handled by others. Breaches of individual privacy can result in different types of harm to individuals, including:

- reputational damage, embarrassment or humiliation
- financial loss, identity theft or fraud
- intimidation, discrimination or physical harm.

More broadly, failing to respect the right to privacy can lead to an erosion of public trust. As such, Ku-ring-gai Council is committed to appropriately handling personal and health information to protect individuals from harm and retain the confidence of the community.

The Privacy Management Plan outlines how Ku-ring-gai Council manages personal and health information in accordance with the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002*. The objectives of the plan are to:

- explain Council's commitment to protecting the privacy of members of the public
- assist Council staff and councillors understand and comply with their legal obligations in managing personal and health information
- describe how members of the public can request access to personal or health information that is held by Council, how it can be amended and how privacy complaints are handled.

The Privacy Management Plan applies to all Council staff and councillors. It also applies to contractors, volunteers and others who are engaged by Council and collect or hold personal or health information.

The Privacy Management Plan outlines how Council works to protect personal and health information in line with legislation and regulatory requirements. Council will aim to ensure that the plan remains compliant with changes to legislation and regulations, but if any part of this plan differs from or conflicts with any applicable law or regulation, the latter will prevail.

Responsibilities

A range of legislation[1] and policies affects how Council handles personal and health information.

Privacy and Personal Information Protection Act 1998

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) outlines how NSW public sector agencies (including councils) are required to manage personal information. Council is required to prepare and implement a Privacy Management Plan under section 33 of the PPIP Act.

The 12 Information Protection Principles (IPPs)[2] are the key to the PIPP Act. These are legal obligations that public sector agencies must follow when collecting, storing, using or disclosing personal information. These principles also give people the right to request access to their personal information or to ask for amendments to that information to ensure it is accurate. Exemptions may apply in some instances, and the Privacy Officer can provide further advice.

Health Records and Information Privacy Act 2002

The *Health Records and Information Privacy Act 2002* (HRIP Act) outlines how NSW public sector agencies (including councils) and health service providers are required to manage the health information of members of the public in NSW.

The HRIP Act includes 15 Health Privacy Principles (HPPs)[3]. Like the IPPs, these are legal duties that describe what NSW public sector agencies and private sector organisations must do when they handle health information.

Government Information (Public Access) Act 2009

The GIPA Act sets out the rules about how members of the public can access government information from NSW public sector agencies.

People may request access to their own personal information, either in its own right or in combination with other government information, or they may seek access to the personal information of other people. Personal information can be both a consideration in favour of

[1] Other NSW legislation includes (but is not limited to): the *Local Government Act 1993* (including provisions under Section 739 relating to suppression of personal information); the *State Records Act 1998* (including the General Retention and Disposal Authority: Local Government Records (GA39)) made under that Act; the *Criminal Records Act 1991* (section 13 prohibits disclosure of spent and quashed convictions); the *Crimes Act 1900* (part 6 includes offences for unauthorised access to or interference with data in computers); the *Independent Commission Against Corruption Act 1988* (the definition of corrupt conduct under section 8 includes the misuse of information held by an agency); and the *Workplace Surveillance Act 2005*.

[2] The full text of the Information Protection Principles is published in Part 2 of the *Privacy and Personal Information Protection Act 1998*.

[3] The full text of the Health Privacy Protection Principles is published in Schedule 1 of the *Health Records and Information Privacy Act 2002*.

disclosure, and a consideration against disclosure. Council will apply these considerations when carrying out the public interest test under the GIPA Act.

Privacy Act 1988 (Commonwealth)

The Commonwealth Privacy Act applies to Australian government agencies and large private entities. Council does not generally have obligations under the Commonwealth Act, but some contracted service providers may have certain duties or exemptions.

Code of Conduct

Under Ku-ring-gai Council's Code of Conduct, all staff must comply with the PIPP Act, the HRIP Act, the privacy principles, the Privacy Management Plan and the Privacy Code of Practice for Local Government. A breach of the Privacy Management Plan is a breach of the Code of Conduct.

Furthermore, corrupt and unlawful disclosure and use of personal information may result in financial penalties or imprisonment[4].

Privacy Officer

The Manager of Governance and Corporate Strategy is Council's Privacy Officer. The Privacy Officer is the point of contact for all matters related to privacy and personal information at Council. Other responsibilities of the Privacy Officer include:

- liaising with the NSW Information and Privacy Commission (IPC) about the implementation of privacy laws, and matters related to privacy and personal information
- disseminating information on privacy issues within Council
- coordinating the steps to be taken by Council to implement privacy laws, including the Privacy Management Plan, privacy notifications and training for staff
- assessing complaints and making recommendations about whether they are about personal information and/or health information
- ensuring that complaints about privacy breaches and/or internal reviews are dealt with in the proper manner.

[4] See Section 664 of the *Local Government Act 1993*, Sections 62-63 of the *Privacy and Personal Information Protection Act 1998* and Sections 68-70 of the *Health Records and Information Privacy Act 2002*.

Promoting privacy

All Council staff should be aware of the Privacy Management Plan and how it applies to their work. All staff should also understand what their obligations are, how to manage personal and health information and what to do if they are uncertain. Council promotes awareness of privacy obligations by:

- publishing the Privacy Management Plan and supporting information on Council's intranet and controlled documents register
- providing information to staff on induction and in refresher training
- providing messages to staff about privacy, including changes to legislation and policy and participating in Privacy Awareness Week
- providing tailored training, advice and support to business units and staff.

When staff members have questions about a privacy matter, they may consult their manager or Council's Privacy Officer.

Council promotes public awareness of Council's Privacy Management Plan by:

- making it publicly available on Council's website
- referring to the Privacy Management Plan in privacy notices and consent forms
- referring to the Privacy Management Plan when responding to enquiries concerning personal and health information.

For Council staff: Privacy by design

Privacy by design aims to ensure that good privacy practices are built into information systems, business processes, products and services. Staff should consider whether a privacy impact assessment is needed when implementing new software, transitioning to cloud-based technologies or other projects that involve the collection, storage, use or disclosure of personal information. An assessment should include the positive and negative impacts on privacy, compliance with legislation and controls to mitigate any risks. Contact the Information Management Team or Privacy Officer for further information.

Reporting on performance and improving practices

The Privacy Officer is responsible for coordinating a self-assessment of privacy culture, governance and practices and identification of improvement actions every two years. Results and recommendations will be reported to the Senior Executive (GMD).

What is personal and health information?

Personal information[5] is any information that identifies an individual and includes:

- written records which include an individual's name, address and other details
- financial information
- photographs, images, video or audio footage
- fingerprints, blood or DNA samples.

Personal information does not include:

- information about an individual that is contained in a publicly available publication
- information about an individual who has been dead for more than 30 years
- information about an individual that is contained in a public interest disclosure, or that has been collected in the course of an investigation arising out of a public interest disclosure
- information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Health information[6] is a specific type of personal information which contains information about an individual's physical or mental health or disability. It includes:

- personal information an individual provides to any health organisation
- a health service provided to an individual
- a health service that is going to be provided to an individual
- a health service an individual has asked to be provided to them
- some personal information for organ donation
- some genetic information about an individual, their relatives or descendants.

[5] "Personal information" is defined in section 4 of the PPIP Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained.
[6] "Health information" is a more specific type of personal information and is defined in section 6 of the HRIP Act.

What personal and health information is collected by Council?

Council collects, stores and uses personal information about ratepayers, residents, customers and other individuals to carry out its functions, deliver its services and comply with State Records requirements. This information includes:

- names, signatures, contact details and dates of birth
- financial and credit information relating to rates, fees and charges
- details relating to property ownership
- applications to access Council programs, services and facilities
- service requests or complaints
- development and other land use applications and objections to applications
- vehicle registration details relating to parking and traffic matters
- photographs and CCTV footage relating to crime prevention
- library lending records and special needs statements
- leases, licences and agreements
- childcare information, immunisation, illness and accident records
- youth health information for excursions
- submissions and information collected as part of Council's community engagement and consultation activities
- other information required by Council to deliver its functions and services.

Council collects, stores and uses personal and health information about councillors and staff, such as:

- names, signatures, personal contact details, postal addresses and dates of birth
- wage and salary entitlements, allowances, leave and payroll data
- driver's license information
- information relating to recruitment, including qualifications, residency or citizenship status, Working with Children Checks, medical history and status
- information relating to performance management and training
- information on complaints and disciplinary matters
- medical certificates and other health information relating to leave and workers compensation
- health histories in relation to immunisation, childcare and disabilities
- photographs and CCTV footage
- disclosure of interest returns
- other information required by Council to deliver its functions and services.

Unsolicited information

Information received by Council where it has not been required or asked for is not subject to the collection principles in the PIPP Act and HRIP Act. However, unsolicited information remains subject to principles relating to storage, access, use and disclosure.

Collection of personal information

Council sometimes needs to collect personal information to carry out its functions and deliver its services. When collecting personal and health information Council aims to ensure that the collection of this information is relevant, proportionate, and respectful of individuals' privacy, avoiding any excessive or unreasonable intrusion. Council must abide by the relevant IPPs when collecting personal information, and the HPPs when collecting health information.

Lawful (IPP1 / HPP1)

Council will only collect personal and health information for a lawful purpose, which is directly related to a function or activity of Council and the collection is necessary for that purpose.

Direct (IPP2 / HPP3)

Council will only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.

Council will only collect health information directly from the person concerned unless it is unreasonable or impracticable to do so.

Open (IPP3 / HPP4)

Council will take reasonable steps to inform the person why personal and health information is being collected, what Council will do with it and who else might see it. Council will take reasonable steps to tell the person how they can view and correct their information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.

If Council collects health information about a person from a third party, it will take reasonable steps to notify the person that this has occurred.

Relevant (IPP4 / HPP2)

Council will take reasonable steps to ensure that personal and health information is relevant, accurate, complete, up-to-date and not excessive. Council will ensure that collection does not unreasonably intrude into the personal affairs of individuals.

For Council staff: Privacy notices

To support compliance with the PIPP Act and HRIP Act, all Council's paper and online forms that collect personal and/or health information must include a privacy notice**.** A privacy notice provides accessible information to individuals about why their information is being collected, how it will be used and who it will be disclosed to. A template is provided below, which should be tailored to meet the requirements of each collection.

Ku-ring-gai Council Privacy Notice

Ku-ring-gai Council (the 'Council') manages privacy and personal information in accordance with relevant legislation and Council's Privacy Management Plan. Your Personal Information is being collected by the Council to facilitate and process your requests and/or to keep you informed about the Council's related activities. Council takes reasonable steps to comply with all relevant legislation and your information will be stored in accordance with relevant legislation and will only be accessed by authorised person(s). You accept the provision of personal information is voluntary, however if you do not provide the information requested, we may not be able to process your request. Information provided by you may be accessed by government agencies and members of the public in accordance with relevant legislation. Ku-ring-gai Council is to be regarded as the agency that holds the information. Under the *Privacy and Personal Information Protection Act 1998* and the *Government Information (Public Access) Act 2009* you can apply to access records of personal information Council holds about you, and then apply to amend or correct personal information by writing to Council's Privacy Contact Officer at Locked Bag 1006 Gordon NSW 2072 or via email at governance@krg.nsw.gov.au. You can view Council's Privacy Management Plan by visiting Privacy Ku-ring-gai (nsw.gov.au).

Notifying a person of what Council intends to do with their information is not the same as seeking their consent. Consent is only required where Council requires an exception to a one of the privacy principles, or authority to handle personal or health information in a particular way. Contact the Privacy Officer for further information.

Storage, access and accuracy of personal information

Council is required to protect the personal information it holds and take reasonable steps to ensure it is accurate, up-to-date and complete. Council must abide by the relevant IPPs when storing personal information, and the HPPs when storing health information.

Secure (IPP5 and HPP5)

Council will store personal and health information securely, keep it no longer than necessary and dispose of it appropriately. It will also be protected from unauthorised access, use, modification or disclosure.

For Council staff: Securing records

All paper records containing personal or health information must be stored in an appropriate, secure location (e.g. a locked room or filing cabinet) when not in use, and disposed of securely (e.g. in lockable bins).

All electronic records must be stored on Council's secure electronic document management system (Content Manager) in line with the Records Management Policy.

Security settings in Content Manager are set as open by default to prevent over-classification and unnecessarily limit access to information.

Security settings for records containing sensitive personal, financial or health information are based on the need-to-know principle[7] to minimise the risk of unauthorised access or misuse of information.

Transparent (IPP6 and HPP6)

Council will take reasonable steps to explain to the person what personal or health information about them is being stored, why it is being used and any rights they have to access it.

Accessible (IPP7 and HPP7)

Council will allow people to access their personal and health information without excessive delay or expense.

[7] The term "need-to-know" means that access to information is limited to business units or positions that need to know or use it. Staff (including contractors) are not entitled to access information merely because it would be convenient for them to know or because of their seniority.

Correct (IPP8 and HPP8)

Council will allow people to update, correct or amend their personal information where necessary. Special considerations may apply to State records.

Members of the public can contact the Customer Service team (by phone on 9424 0000 or email at krg@krg.nsw.gov.au) for advice on how to access, update or correct their contact details or other personal information stored by Council.

Accurate (IPP9 and HPP9)

Council will take reasonable steps to make sure that personal and health information is relevant and accurate before using it.

This may include training staff on proper data handling, checking and validating data when it is collected and addressing any identified errors or discrepancies. Council's records management systems provide a robust system of controls and allow Council to track any changes made to the data.

Use and disclosure of personal information

Personal information will generally only be used for the purpose it was collected for. Council must abide by the relevant IPPs when using or disclosing personal information, and the HPPs when using or disclosing health information.

Limited (IPP10 and HPP10)

Council will only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious and imminent threat to any person's health or safety[8].

Council will only use health information for the purpose it was collected or for a directly related purpose that a person would expect. Otherwise, Council will need their consent to use the health information for a secondary purpose.

Restricted (IPP11 and HPP11)

Council will only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety[9].

Council will only disclose health information for the purpose for which it was collected, or for a directly related purpose that a person would expect. Otherwise, Council will need their consent.

Safeguarded (IPP12)

Council will not disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It would only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

[8] Council may use personal information for a purpose other than for which it was collected if it is reasonably necessary for Council's lawful and proper functions. Refer to section 4.11 of the Privacy Code of Practice for Local Government.

[9] Refer to Council's Compliance Policy for circumstances under which personal information may need to be disclosed when Council is investigating allegations of unlawful activity.

Other limits on health information (HPP12-15)

Council will give a person the option of receiving health-related services anonymously, where this is lawful and practicable.

Council will only identify people by using unique identifiers if it is reasonably necessary to carry out functions efficiently.

Council will only transfer health information outside New South Wales in accordance with HPP14 in Schedule 1 of the HRIP Act. Council will only use health records linkage systems if the person has provided or expressed their consent.

De-identification of personal information

De-identification enables information to be used while preserving an individual's privacy. Council may redact or remove identifying information from documents or data prior to publication or release to a third party. If the identity of the person is no longer apparent or cannot be reasonably ascertained from the information or data, then it is not personal information for the purposes of the PIPP Act.

Data sharing

Council engages the services of third-party providers and contractors and may need to share data containing personal information to deliver a service. Council may also share data with NSW government agencies for specific purposes set out in the legislation.

Council takes appropriate measures to safeguard the security and confidentiality of personal information it may be required to share. Council carefully selects providers who can demonstrate compliance with NSW privacy laws and industry standards, establishes clear contractual obligations regarding data protection, and monitors compliance with these requirements. Council will only share personal information in accordance with this policy, the PPIP Act, HRIP Act and any applicable Public Interest Direction or Privacy Code of Practice.

Data breaches and notifications

A data breach occurs when a failure leads to or potentially leads to unauthorised access to an organisation's data. This may result from human or technical error, malware, hacking or data theft. Some data breaches are serious and can cause significant harm to organisations and individuals.

Council has controls in place to protect the information it holds, and response strategies should these controls ever fail. See Council's Information and Cyber Security Policy and Cyber Incident Response Plan for further information.

NSW does not currently have a mandatory notifiable data breach reporting requirement[10]. However, in the event of a serious breach (one that puts the safety of individuals at risk, leads to financial loss or reputational damage, or releases commercially sensitive information) Council will notify affected individuals / organisations as quickly as possible so they can take the steps required to protect themselves from harm.

Complaints by staff alleging breaches of the PIPP Act, the HRIP Act or the Privacy Management Plan should be made in writing to the General Manager.

[10] Privacy and Personal Information Protection Amendment Act 2022 will introduce a mandatory notification of data breach scheme into NSW. The Act is to commence in November 2023.

Exemptions to the PIPP Act

There are a number of exemptions to the PIPP Act in the legislation itself, in privacy codes of practice and public interest directions[11] made by the NSW Privacy Commissioner. These exemptions allow Council to modify the application of the IPPs in certain circumstances.

The PIPP Act[12] includes several exemptions from the principles relating to:

- law enforcement, intelligence and investigative agencies
- legal proceedings and court orders
- where non-compliance is authorised, permitted under another law or would benefit the individual concerned
- exchange of information between public sector agencies
- research or compilation of statistics
- credit information
- emergency situations.

Council is exempt[13] from sections of the PIPP Act relating to the collection of personal information by CCTV camera installed in a public place. Council may also disclose this personal information to the NSW Police Force by way of live transmission from a CCTV camera.

The Privacy Code of Practice for Local Government also modifies some of the IPPs:

- Council is not required to comply with the IPPs where indirect collection of personal information is reasonably necessary for issuing an award, prize, benefit or similar form of personal recognition[14].
- Council may disclose personal information to public sector agencies or utility providers if they have approached Council in writing, and Council is satisfied that sharing this information is reasonably necessary and will be properly used[15].
- Where requested by a potential employer, Council may verify that a current or former employee works or has worked for Council, the duration of their employment, and the position occupied during their employment. Council may only give an opinion on their suitability to the position if Council is satisfied the person has provided consent for Council to provide a reference[16].

[11] Under section 41 of the *Privacy and Personal Information Protection Act 1998*, the Privacy Commissioner, with the approval of the Attorney General, may make a Public Interest Direction to waive or make changes to the requirements for a public sector agency to comply with an Information Protection Principle. There are no directions currently in operation that apply to Council.
[12] Refer to sections 22-28 of the *Privacy and Personal Information Protection Act 1998*.
[13] Refer to Clause 9 of the *Privacy and Personal Information Protection Regulation 2019*.
[14] Refer to the Privacy Code of Practice for Local Government for details. This exemption applies to IPPs 2, 3, 10 and 11.
[15] This exemption applies to IPP11.
[16] This exemption applies to IPPs 11 and 12.

Public registers

A public register is an official list of names, events and transactions that must be made available to the public. Open access public registers[17] on Council's website include:

- development applications (DAs) and associated documents, certificates and reports (on DA Tracking)
- information on applications for construction certificates (CCs) and complying development certificates (CDCs) (on DA Tracking)
- the Council land register (link)
- Council's contract register (link)
- agendas and business papers for Council meetings and committees (link)
- declaration of interest returns of councillors (link) and designated officers (link)
- the register of councillor voting on planning and development matters (link)
- the register of approved variations from local development standards (link)
- development contributions register (link)
- planning agreement register (link)

Registers available online do not generally include personal information.

Other open access records that may contain personal information and will be made freely available under an informal access to information (GIPA) request include:

- documents and plans relating to CCs and CDCs
- records of approvals relating to water supply, sewerage and stormwater works, waste management, use of community land and other activities requiring Council approval[18]
- orders, notices and directions relating to food safety, environmental protection, public health, road safety and other matters that Council regulates[19]
- Council's register of graffiti removal works[20]
- leases and licences for use of community land
- Council's GIPA disclosure log[21].
- investments register

[17] Schedule 1 of the *Government Information (Public Access) Regulation 2018* prescribes certain records held by local authorities as open access. Open access information and registers must be made freely and publicly available.
[18] Activities requiring the approval of council are listed in section 68 of the *Local Government Act 1998.* The requirement to maintain a record of approvals is described in section 113.
[19] Schedule 1, clause 4 of the *Government Information (Public Access) Regulation 2018* prescribes orders given by local authorities under Part 2 of the Local Government Act 1993 or any other Act as open access..
[20] Kept in accordance with section 13 of the *Graffiti Control Act 2008*
[21] Section 25 of the GIPA Act requires agencies to keep a disclosure log that records information about access applications made to the agency that the agency has decided to provide access to and may be of interest to other members of the public.

Because every public register is different, the type of personal information that may be included on each register depends on the purpose and situation. Personal information kept on public registers may include:

- names, signatures, contact details and dates of birth
- details relating to property ownership and insurance
- development and other land use applications and objections to applications
- other information relating to the register's purpose or required under the Act.

Personal information may be included on a public register if Council is satisfied that it is required by the relevant laws and/or will be used for a reason relating to the purpose of the register.

Personal information about a person will not be released to another person unless it is contained within a public register (or other exceptions apply under legislation).

Council may de-identify or exclude personal information from documents on a public register or made available under an access to information (GIPA) request if it is not required under law and it is practical to do so.

Council may require any person who applies to inspect personal information contained in a public register to give particulars (in the form of a statutory declaration) as to the intended use of any information obtained from the inspection.

Suppression of personal information contained in a register

Where someone's safety or wellbeing may be affected, a person may ask that personal information is removed from a public register or not released to the public[22].

Council must suppress the information if it is satisfied that the safety or wellbeing of a person would be affected and is not outweighed by the public interest in maintaining open access to the information.

Applications to suppress personal information from a public register should be made in writing to the Privacy Officer and include any relevant supporting documentation.

[22] Refer to section 58 of the *Privacy and Personal Information Protection Act 1998*.

Privacy complaints

If a person believes that Council has misused their personal or health information they can make a complaint, ask for an internal review or complain to the NSW Privacy Commissioner.

Informal complaints

Most minor privacy concerns can be resolved quickly and easily through Council's informal complaint handling procedure. Feedback and complaints forms are available on Council's website here. Council's Complaints Management Policy (link) provides further detail on how complaints will be managed and resolved.

Internal review

Individuals have the right to seek an internal review if they believe that Council has mishandled their own personal and health information.

An internal review is a fact-finding investigation into the privacy complaint. The complaint must be about conduct where Council has breached one or more privacy principles (or an exemption to the privacy principles such as the Local Government Privacy Code of Practice).

Applications for an internal review should be addressed (in writing) to Council's Privacy Officer. It must be made within six months from the time the applicant first became aware of the conduct.

Council's Privacy Officer will conduct the internal review[23]. Council will endeavour to acknowledge receipt of the complaint within five working days and complete the internal review within 60 days. Following the review, Council may do any one or more of the following:

- take no further action on the matter
- make a formal apology
- change practices and/or provide training to staff to ensure that the conduct does not happen again
- take appropriate remedial action.

The applicant will be informed of the findings of the review, the action that Council proposes to take (if any), and further rights of review.

[23] If the internal review is about the Privacy Officer, the General Manager will appoint another officer to conduct the review.

The Privacy Commissioner's role in internal reviews

Council must keep the Privacy Commissioner informed of an internal review application and its progress until it is finalised.

The Commissioner has an oversight role in how Council handles privacy complaints. The Commissioner may make submissions in relation to an internal review and Council is to consider any relevant material submitted by the Commissioner.

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

If the internal review is not completed within 60 days, applicants are entitled to make an application under section 55 of the Act to the NSW Civil and Administrative Tribunal (NCAT) for a review of the conduct concerned.

An applicant may also seek a review by the NCAT if they are not satisfied with the action taken in relation to an application for an internal review.

Contacts

Ku-ring-gai Council Privacy Officer

The Manager of Governance and Corporate Strategy is Council's Privacy Officer. The Privacy Officer is the point of contact for all matters related to privacy and personal information at Council.

The Privacy Officer (Manager Governance and Corporate Strategy)
Email: governance@krg.nsw.gov.au
Telephone: (02) 9424 0000
Address: 818 Pacific Highway, Gordon NSW 2072
Postal: Ku-ring-gai Council, Locked Bag 1006, Gordon NSW 2072

NSW Information and Privacy Commission

The Information and Privacy Commission (IPC) is an independent statutory authority that administers NSW's legislation dealing with privacy and access to government information.

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

Abbreviations and definitions

Term / abbreviation	Definition
Council staff	Councillors and employees of Council (full-time, part-time, temporary or casual). For the purposes of the Privacy Management Plan, it also includes people engaged by Council in a paid or unpaid capacity (including contractors, committee members, Council owned business operators, work experience participants, volunteers, student placements and family day carers).
De-identification	Removal of identifiers from personal information so that a person's identity is no longer apparent or cannot be reasonably ascertained from the information or data (e.g. redacting names, addresses and telephone numbers).
Government Information (Public Access) Act 2009 (GIPA Act)	The NSW law sets out how citizens can access government information from NSW government agencies.
Health information	Personal information that is information or an opinion about the physical or mental health or a disability of an individual, an individual's express wishes about the future provision of health services to him or her, a health service provided (or to be provided) to an individual. Also includes personal information collected to provide a health service, in connection with organ donation, or genetic information that could be predictive of the health of an individual or genetic relative, or healthcare identifiers. For a full definition, see section 6 of the *Health Records and Information Privacy Act 2002*.
Health Privacy Principles (HPPs)	The legal obligations which NSW public sector agencies and private sector organisations must abide by when they collect, hold, use and disclose a person's health information. These are set out in Schedule 1 of the *Health Records and Information Privacy Act 2002*.
Health Records and Information Privacy Act 2002 (HRIP Act)	The NSW law that outlines how NSW public sector agencies (including councils) and health service providers are required to manage the health information of members of the public in NSW.
Health service	Includes medical, hospital, nursing and midwifery services, dental services, mental health services, pharmaceutical services, ambulance services, community health services, health education services and other services defined in section 4 of the *Health Records and Information Privacy Act 2002*.
Identifier	A number or other identifier assigned to an individual in relation to their health information by an organisation for the purpose of uniquely identifying that individual.
Information and Privacy Commission (IPC)	The independent statutory authority that administers legislation dealing with privacy and access to government held information in NSW.
Information Protection Principles (IPPs)	The legal obligations which NSW public sector agencies, statutory bodies, universities and local councils must abide by when they collect, store, use or disclose personal information. These are set out in Division 1 of Part 2 of the *Privacy and Personal Information Protection Act 1998*.
Internal review	An internal assessment of conduct in response to a complaint. Under section 53 of the *Privacy and Personal Information Protection Act 1998*, a person who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct.

NSW Civil and Administrative Tribunal (NCAT)	The NSW tribunal that decides a range of civil and administrative cases, including reviews of decisions and the conduct of government agencies relating to privacy and personal information or health records and information.
Personal information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. For a full definition, see section.4 of the *Privacy and Personal Information Protection Act 1998*.
Privacy and Personal Information Protection Act 1998 (Act)	The NSW law that outlines obligations to protect the personal information agencies collect about individuals and responsibilities for the management and handling of personal information.
Privacy notice	Information provided to individuals when collecting information about how personal information may be used.
Privacy Officer	The staff member responsible to assist the application of *the Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002* within their own organisation.
Public register	A register of personal information that is required by law to be, or is made, publicly available or open to public inspection (as defined under section. 3 of the *Privacy and Personal Information Protection Act 1998)*.
Sensitive information	Personal information that is also information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities (see section 19 of the *Privacy and Personal Information Protection Act 1998)*.