Shoalhaven City Council

1300 293 111 | shoalhaven.nsw.gov.au

Privacy Management Plan

Adoption Date:	25/06/2007
Amendment Date:	14/11/2022
Minute Number:	MIN07.837, MIN09.1139, MIN13.846, MIN22.862
Review Date:	14/11/2025
Directorate:	City Performance
Record Number:	POL23/8 (10357e)

Contents

Preface

The *Privacy and Personal Information Protection Act 1998* (the "PPIPA") requires all councils to prepare a Privacy Management Plan (Plan) outlining their policies and practices to ensure compliance with the requirements of that Act and the *Health Records and Information Privacy Act 2002* (the HRIPA).

In particular, the object of this plan is to inform:

- The community about how their personal information will be used, stored and accessed after it is collected by the Council; and
- Council staff of their obligations in relation to handling personal information and when they can and cannot disclose, use or collect it.

WHAT THIS PLAN COVERS

The Shoalhaven Council (the Council) is required to have a Plan under s33 of the PPIP Act which must include:

- information about how the Council develops policies and practices to ensure compliance with the PPIP Act and the HRIP Act
- how employees are made aware of these policies and practices
- the Council's internal review procedures anything else the Council considers relevant to the Plan in relation to privacy and the personal and health information it holds.

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

WHEN THIS PLAN WILL BE REVIEWED

This Plan will be reviewed every two years. It will be reviewed earlier if any legislative or administrative changes affect the management of personal and health information by the Council.

1. Introduction

The *Privacy and Personal Information Protection Act 1998* [PPIPA] section 33, requires all public-sector agencies to prepare, implement and review their *Privacy Management Plan* at least every three years. This policy also outlines how Shoalhaven City Council complies with the legislative requirements of the PPIPA, the *Health Records and Information Privacy Act 2002* [HRIPA] and the *Privacy Code of Practice for Local Government* [the Code].

Shoalhaven City Council (the Council) is committed to protecting the privacy of our customers, business contacts, Councilors, employees, contractors, and volunteers. This Privacy Management Plan (Plan) aims to ensure Council manages the personal and health information it collects, stores, accesses, uses and discloses in the course of its business activities ethically and appropriately.

This Plan is designed to inform the community and educate staff on access to personal information and to introduce Council policies and procedures to maximise compliance with the PPIPA and the HRIPA. This Plan also outlines how Council will incorporate the 12 Information Protection Principles (available at the below link) into its everyday functions:

https://www.ipc.nsw.gov.au/information-protection-principles-ipps-agencies

Where the Council has the benefit of an exemption, it will nevertheless describe procedures for compliance in this Plan. By doing so, it is not to be bound in a manner, other than that prescribed by the Codes.

1.1. What is Personal Information?

Personal information is defined in Section 4 of the PPIPA as:

"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."

Personal information can include a person's name and address, details about their family life, their sexual preferences, financial information, fingerprints, and photos.

1.2. What is not Personal Information?

Personal information does not include information about an individual that is contained in a publicly available publication. Personal information, once it is contained in a publicly available publication, ceases to be covered by the PPIPA.
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 or an opinion about a person's suitability for employment as a public sector official.

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

- a document in a library, art gallery or museum
- State records under the control of the NSW State Archives and Records

- public archives (within the meaning of the Copyright Act 1968 (Cth))

Other information that is not considered personal information for the purposes of PPIPA can be found in Part 4(3) of the PPIPA.
Council considers the following to be publicly available publications:

- An advertisement containing personal information in a local Councillor 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.

In accordance with the GIPAA, when inviting public submissions, Council will advise people that their submission, including any personal information in the submission, may be made publicly available.

Information published in this way ceases to be covered by the PPIPA. Council's decision to publish in this way must be in accordance with PPIPA.

1.3. What is Health Information?

Health information is a more specific type of personal information and is defined in s6 of the HRIP Act. Health information can include information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided to a person.

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

1.4. Why do we Collect Personal and Health Information

Council collects personal information in a variety of ways in order to efficiently perform the services and functions we deliver to the City of Shoalhaven. 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 we collect and manage. Council ensures that both personal and health information is relevant, accurate, is not excessive and does not unreasonably intrude into people's personal affairs.

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. This may occur when a contractor needs to contact a property owner to notify them of an outage or to access their property.

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

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

1.5. How do we collect Personal Information?

Council collects personal information in a variety of ways including:

- incident reports
- medical assessment reports
- submissions
- application forms
- CCTV footage
- financial transaction records
- contracts
- customer enquiries and correspondence
- telematics
- web services and smart devices (the Internet of Things)
- contact tracing under NSW Public Health Orders.

1.6. How do we collect Health Information?

Council collects health information in a variety of ways including:

- incident reports
- medical assessment reports application forms
- phone conversations for example those regarding debt recovery and personal circumstances around hardship
- Seniors' services where information may be collected on medical or support needs;
- • Information on carers and families for the purposes of children's services;
- • Information on personal health and fitness for the purposes of gym membership;
- • Volunteer programs where volunteers are asked to disclose health conditions which assist Council to provide support in the event of an incident or which may preclude them from some types of volunteer work;
- • Information in relation to the need for assisted waste services;
- • Information relating to staff health, for example medical certificates and workers' compensation, fitness for duty assessments; and
- • Medical certificates to the extent that they relate to public liability claims.

Council does not assign unique identifiers for health information.

1.7. Application of this Plan

The PPIPA, the HRIPA and this Plan apply, wherever practicable, to:

- Councillors,
- Council employees,
- Consultants and contractors of the Council,
- Volunteers,
- Council owned businesses; and
- Council Committees (including those which may be established under section 355 of the Local Government Act 1993 (LGA)).

1.8. Personal & Health Information held by Council

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

Councillors

Council holds personal information concerning Councillors, such as:

- Personal contact information
- Complaints and disciplinary matters
- Pecuniary interest returns
- Entitlements to fees, expenses and facilities.

Customers, ratepayers, and residents

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

- Rates records
- Development applications and related submissions
- Library lending records and special needs statements
- Leases, licences and agreements
- Waste services records
- Customer requests
- Fitness testing records
- Burial and cremation records
- Financial records
- Donation, grant and sponsorship applications
- Photos of vehicle registration plates
- Responses to clean up notices regarding health issues
- Youth health information for excursions
- Membership, financial details, member fitness medical records – Leisure Centres
- Childcare information, immunisation, illness and accident records
- Community service utilisation e.g. Community Transport
- Age & disability support records including health records
- Submissions and information collected as part of Council's community engagement and consultation activities
- Public access forum applications
- CCTV footage.

Employees, volunteers, and contractors

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

- Personal contact information
- Recruitment material
- Pre-employment medical information
- Bank account details
- Wage and salary entitlements
- Leave and payroll data
- Employee immunisation records and medical certificates
- Volunteers' medical information
- Disclosure of interest returns
- Workers' compensation investigations
- Public interest disclosure investigations
- Performance management plans
- Disciplinary matters

1.9. Unsolicited Information

Unsolicited information is personal, or health information received by the Council in circumstances where the Council has not asked for or required the information to be provided. Such information is not deemed to have been collected by the Council but the access, storage, use and disclosure Information Protection Principles in this Plan 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, will be treated the same as any other submission and be made available for release to the public.

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 Council for public viewing.

1.10. Applications for suppression in relation to general information (not public registers).

Under section 739 of the Local Government Act 1993 ("LGA") a person can make an application to suppress certain material that is available for public inspection in circumstances where the material discloses or would disclose the person's place of living if the person considers that the disclosure would place the personal safety of the person or their family at risk.

Section 739 of the LGA relates to publicly available material other than public registers. As such, it limits disclosure in those circumstances where an application for suppression is successful. An application for suppression must be verified by statutory declaration and otherwise meet the requirements of section 739. When in doubt, Council will err in favour of suppression.

For more information regarding disclosure of information (other than public registers) see the discussion of IPPs 11 and 12 in Part 3 of this Plan. For information regarding suppression of information on *public registers*, see Part 2 of this Plan.

1.11. Privacy Protection and you

Under s10 of the PPIP Act, when the Council collects personal information from an individual, such as their name, address, telephone number or email address, the 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
- the name and address of the agency that is collecting the information and the agency that is to hold the information (the Council is a public sector 'agency' under s10 of the PPIP Act).

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

Where possible, individuals providing personal information will be given the opportunity to consent to the terms of the Privacy Protection Notice and, in particular, be provided with an 'opt out' check box for 'Other uses', for such additional uses of the personal information as are considered reasonably necessary by the Council for the exercise of Council functions.

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

1.12. Storage, Access and accuracy of personal information & health information

Personal information and health information are both sensitive information and are stored electronically and in hard copy files. The following applies to information the Council holds:

- only authorised Council employees and authorised third parties can access personal information,
- employees will take reasonable steps to ensure personal information is accurate before using it,
- a person may access or request the amendment of personal and health information the Council holds about them by contacting Council's Customer Experience Team.,
- personal information will be kept no longer than necessary and disposed of appropriately in accordance with Council's Records Management Policy.
- reasonable steps to ensure accuracy include collecting the information directly from the individual wherever possible, reconfirming details and maintaining up to date databases.

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

Electronic information will be stored on secure information systems that require individual logins. In addition Council's record management system allows for access controls to be applied to ensure only authorised staff can access sensitive information. New systems will be assessed for compliance with the PPIP Act and HRIP Act. Hard copy files and sensitive information will also be securely stored.

1.13. Use and disclosure of personal information

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

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

Employees use the personal information collected to:

- deliver services,
- conduct research,
- provide advice,
- continually improve services.

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

The Council does not disclose personal information without consent, unless the disclosure is:

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

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

1.14. How we Manage Personal and Health Information Collected and Held by Council

As outlined elsewhere in this Plan Council collects and manages information from a multitude of sources and will always do so in accordance with the PPIP Act. We also endeavour to make as much information available, to individuals whose information we collect/hold, at the time of collection. Additional information is detailed below for services / functions that

frequently collect personal information or manage significant amounts of personal information or data.

Requests for Service, Enquiries and Correspondence

Council receives a significant number of requests for service, as well as general enquiries and
correspondence, and a certain amount of 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 phone (Council does record telephone conversations but allows callers to opt out; and it does have a voicemail service)
- in writing (e-mail, letter, fax, online form)
- in person (at Council's Customer Service Centre or other 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 we 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

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.

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, however, 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.

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 on request, so make sure you read Council's privacy statement before you comment on a Development Application. The up to date privacy statement is available on Council's website.

Staff and Recruitment

Council collects personal and/or health information from staff members as well as part of our 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 and copies of licences essential to the performance of an officer's role

Recruitment

When people apply for jobs at Council, they send us personal information, including their name, contact details and work history. Council provides this information to the interview panel for that particular position in electronic or hard copy files. The personal information is only used for the purposes of the recruitment process. After recruitment is 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 contacts and any disabilities that may impact their work. These forms are sent to the Organisational Development Unit to be used for employment purposes, such as payroll and setting up personnel files and the information is retained in secure storage systems.

Visitors and members of the public (incl. QR Codes)

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 maybe recorded in a physical sign-in register or via a digital QR Code check-in process. During periods of health emergencies, such as during a pandemic Council may provide check-in data for a facility to NSW Health, or any other relevant government agency, for the purposes of maintaining and supporting community health and safety. 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 Corporate Records Management Policy. Check-in data collected by the Service NSW QR Code Check-In system will not be held by Council and will be held and stored by Service NSW.

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 e-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 kept separate from each other and each is 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 our decision-making and the provision of services. Council conducts the majority of its public consultation activities via our "Get Involved" website. We collect information from you when you register to use this site. This includes your email address and additional demographic information as provided by you on the registration form. We collect information about your usage of the site, such as pages visited, documents downloaded, etc.

We collect this information in order to:

- analyse and interpret it to help meet our 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 our providers may have access to your personal information to facilitate services on behalf of Council. Council ensures that our providers adhere to the same legislative requirements in relation to Privacy as well as meet the requirements of this Plan.

Cookies

Council uses 'cookie' technology to collect additional website usage data 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.

Council uses cookies for the following purposes:
- to better understand how you interact with our services
- to monitor aggregate usage by our users and web traffic routing on our services
- to improve our services. Most internet browsers automatically accept cookies.

You can restrict that by editing your browser's 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 Council newsletters etc. To facilitate this our 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 our providers adhere to the same legislative requirements in relation to Privacy as well as meet the requirements of this Plan.

Social Media

We use social networking services such as Twitter, Facebook, LinkedIn and YouTube, 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. Our use of social media sites also involves listening to social trends and issues that relate to Council services and events. We use various tools to view public social media and website commentary in which Council's accounts may not necessarily be tagged – and engage directly with members of the public to provide information or a better level of customer service. In doing so, we 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 collected 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 and we recommend you read these also.

The Internet of Things

The Internet of Things (IoT) is a broad term that generally refers to physical devices connected to the internet that collect, share or use data. IoT devices and the data they collect can provide convenience, efficiency and insights into essentially every aspect of our world. For Council, in coming years, the IoT will provide many benefits and has the potential to generate great public value. These large collections of data can, in many cases, constitute personal, health and sensitive information. Given the passive nature of many IoT devices it can be difficult for individuals to ascertain if their personal information is being collected by an IoT device. For example if "smart bin" technology is introduced it is not possible to have a privacy collection notice on every bin in the city. Council will provide details of what data it collects and what the data will be used for and who it will be shared with, for future IoT devices as they are established. However, this will most likely occur via centralised methods, such as the Council website, rather than at each device or collection point. Council will not

use any personal information without permission and will use collated and de-identified data instead.

2. Public Registers

2.1. Definition

A public register is defined in section 3 of Part 1 of the PPIPA as:

"a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)".

Part 6 of the PPIP 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.

Disclosure in relation to all other personal information must comply with the *Information Protection Principles* as outlined in Part 2 of this Plan and the Privacy Code where it includes personal information that is not published.

Council holds public registers under the *Local Government Act 1993*, including:

- Section 53 - Land Register
- Section 113 - Records of Approvals,
- Section 440AAB - Register of Returns - Pecuniary Interests,
- Section 602 – Record of Rates & Charges,
- Section 319 - Local Government Register of Political Donations,
- Section 328A - Register of Political Donation Disclosures,
- Section 375A - Planning Register,
- Contracts over $150,0000 awarded by Council,
- Non-residential roll,
- Register of investments,
- Register of Contributions,

Council holds public registers under the *Environmental Planning and Assessment Act 1979* [EPA]:

- Section 4.58 – Register of consents and Certificates.

- Council holds a public register under the *Protection of the Environment Operations Act 1997* [POEO] which can be accessed, on request, through Council's Information Officer: Section 308 & 309– Public register of licences held.

Council holds a public register under the *Impounding Act 1993* [IA] which can be accessed, on request, from the Council's Information Officer:

- Section 30 & 31 – Record of impounding.

Members of the public may enquire only in accordance with the primary purpose of any of these registers. The primary purpose for each of these public registers is set out in the section that follows.

2.2. Public Registers, the PPIPA and the HRIPA

A public register generally confers specific rights or privileges, a benefit, or status, which would not otherwise exist. It may be required by law to be made publicly available or open to public inspection, or it is simply made publicly available or open to public inspection (whether or not payment is required).

Section 57 of the PPIPA requires very stringent controls over the disclosure of personal information contained in a public register. It provides broadly that where Council is responsible for keeping a public register, it will not disclose any personal information kept in that register unless it is satisfied that the information is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

Section 57 (2) provides that in order to ensure compliance with section 57(1), a Council may require any person who applies to inspect personal information contained in the public register to give particulars in the form of a statutory declaration as to the proposed use of that information.

Registers should not be published on the internet.

2.3. Applications for Suppression in Relation to a Public Register

A person about whom personal information is contained (or proposed to be contained) in a public register, may request Council under section 58 of the PPIPA to have the information removed from, or not placed on the register.

If Council is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, Council will suppress the information in accordance with the request.

An application for suppression should be made in writing and addressed to the Chief Executive Officer. It must contain sufficient detail to allow for the proper assessment of the application and supporting documentation may be required.

2.4. Application for access and to amend own personal and health information

Council will at the request of the individual concerned, consider any request to alter or amend information held, 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.
Council does not charge a fee to access and amend personal and health information.

If you wish to access or amend your personal and/or health information the Council holds, such as your contact details please phone 1300 293 111 or use the make a request function on our website.
We will direct your enquiry to the applicable area of the organisation or the Information and Privacy Officer. If necessary, Council will seek verification of your identity.

Where substantive amendments are involved, a written application will be required.

The application should set out the grounds on which changes are sought.
Council may refuse to amend information where it is not satisfied that it is incorrect or incomplete.
If Council refuses a request for amendment, the individual may request a notation to be added to the record.
If information in a Council record is amended, the person is entitled, if practicable, to ensure other authorised staff are notified of the amendments.

Limits on accessing or amending information:
Council is prohibited from providing one person access to another person's personal and health information.
However:
– under s26 of the PPIP Act, a person can give the Council consent to disclose their personal information to someone that would not normally have access to it;
– under s7 and s8 of the HRIP Act, an "authorised person" can act on behalf of someone else; and
– the Council may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual, to find a missing person or for compassionate reasons.

2.5. How do I amend my own personal or health information?

Individuals wanting to a amend their own personal or health information must put the request to Council via email council@shoalhaven.nsw.gov.au or by phone 1300 293 111. 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 PPIP Act or HRIP Act
- Explain what personal or health information the person wants to amend
- Confirmation of the applicant's identity.

2.6. Limits on accessing or amending own personal and health information

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

- under s26 of the PPIP Act, a person can give the Council consent to disclose their personal information to someone that would not normally have access to it;
- under s7 and s8 of the HRIP Act, an "authorised person" can act on behalf of someone else; and
- the Council may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of the individual, to find a missing person or for compassionate reasons.

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

- accidental loss or theft of information or equipment on which such information is stored (e.g., loss of a paper record, laptop or USB stick)
- unauthorised use, access to or modification of data or information systems to gain unauthorised access or make unauthorised changes to data or information systems –

accidental or unauthorised disclosure of personal information (e.g., email containing personal information sent to incorrect recipient)
- personal information posted on the Council 's website without consent
- access to Council data by an authorised system user for unauthorised reasons (e.g., a Council employee looking up information in a corporate records management system for personal reasons in breach of the Council 's Code of Conduct)
- accidental disclosure of user login details 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. Responding to a data breach

The Director City Performance, the Manager Business Assurance & Risk, the Chief Information Officer or the Unit Manager IT Support, must be promptly informed of any data breach and will assist in the assessment and management of the breach, including any reporting under NSW's voluntary data breach reporting scheme, in accordance with the Information and Privacy Commission's Voluntary Data Breach Notification guidelines:

. https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification

The Council determines whether personal information has been accessed and/or disclosed to determine what response should be taken. The Council 's default position is to voluntarily report data breaches to the Privacy Commissioner.

The Council will determine the seriousness of a breach by:
- considering the type of data held,
- whether personal or health information was disclosed,
- the number of individuals affected,
- the risk of harm that could be caused to both individuals and the Council by the breach.

4. Review Rights and Complaints

The Council encourages the informal resolution of privacy issues before undertaking the review process. Issues can be raised informally with the Council and complaints will be managed under the Council's Complaints Policy and Procedures. Further details on the Council's complaints and feedback procedures can be found on the Council's website.

4.1. Internal review

Individuals have the right to seek an internal review under Part 5 of the PPIP Act if they believe that the Council has breached the PPIP Act or HRIP Act relating to their own personal and health information. Individuals cannot seek an internal review for a breach of someone else's privacy, unless they are authorised representatives of the other person. An internal review is an internal investigation that the Council conducts into a complaint. The Council will assess whether or not it has complied with its privacy obligations, and then tell the applicant of its findings and if it will take any further action.

4.2. Internal review process

Applications for an internal review must:

- be in writing – be addressed to the Council's Public Officer - Manager – Business Assurance & Risk,
- specify a postal or email address in Australia to which the Council may send its review response,
- be made within six months from first becoming aware of the conduct that is the subject of the application.

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

The Public Officer, or their delegate, will conduct the internal review. If the internal review is about the conduct of the Privacy Contact Officer, the Director City Performance will appoint another person to conduct the internal review.

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

The Council aims to:

- acknowledge receipt of an internal review within 5 working days,
- complete an internal review within 60 calendar days.

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

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

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

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

4.3. The Privacy Commissioner's role in internal reviews

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

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

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

- inform the Privacy Commissioner of the findings of the review and the action proposed to be taken by the Council in relation to the matter.

The Council must notify the applicant of the outcome of the review within **14 days** of its determination. A copy of the final review should also be provided to the Privacy Commissioner where it departs from the draft review.

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

An internal review checklist has been prepared by the Office of the Privacy Commissioner NSW and can be accessed from its website:

http://www.ipc.nsw.gov.au.

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

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

4.5. Promoting Privacy

Compliance strategy

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

Council officials will be regularly acquainted with the general provisions of the PPIPA and HRIPA and, in particular, this Plan, the Information Protection Principles, the Public Register provisions, the Privacy Code of Practice for Local Government, and any other applicable Code of Practice.

Communication Strategy

Council will promote awareness of this plan and rights under PPIPA, HRIPA and this Plan to Council officials by:

- Publishing the plan on our internal and external websites
- Providing specialised and on-the-job training to key groups

Promoting the Plan to the Community

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

- Making it publicly available and publishing it on our website
- Writing the Plan in plain English
- Provide a link on our website to the Information & Privacy Commission website and distributing copies of literature available on that site

- Including privacy statements on application forms and invitations for community engagement

5. Managing Personal and Health Information under Legislation

This section contains a general summary of how the Council must manage personal and health information under the *Privacy and Personal Information Protection Act 1998* (PPIP Act), the *Privacy and Personal Information Protection Regulation 2019*, the *Health Records and Information Privacy Act 2002* (HRIP Act) and other relevant legislation.

5.1. The Privacy and Personal Information Protection Act

The PPIP Act sets out how the Council must manage personal information. Information protection principles Part 2, Division 1 of the PPIP Act contains 12 Information Protection Principles (IPPs) with which the Council must comply. The following is an overview of the principles as they apply to the Council.

Collection

The Council collects personal information only for a lawful purpose that is directly related to the Council ’s functions and activities.
The Council collects personal information directly from the person concerned. The Council will not collect personal information from third parties unless the individual has authorised collection from someone else or, in the case of information relating to a person under the age of 16 years, the information has been provided by a parent or guardian.
The Council informs people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. The Council will tell people how they can access and amend their personal information and any possible implications if they decide not to give their personal information to us.
The Council ensures that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into people’s personal affairs.

Storage

The Council will store personal information securely, keep it no longer than necessary and dispose of it securely and in accordance with the Council ’s obligations under the State Records Act 1998 and any other requirements for the retention and disposal of personal information. Personal information is protected from unauthorised access, use or disclosure.

Access and accuracy

The Council is transparent about the personal information it holds, why it is used, and the right to access and amend it.

The Council allows people to access their own personal information without unreasonable delay or expense..

The Council allows people to update, correct or amend their personal information where it is necessary.

The Council will take reasonable steps to ensure that personal information is relevant and accurate before using it.

Use

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

The Council does not disclose personal information without consent, unless disclosure is:
- for a purpose directly related to the reason we collected it, and where Council has no reason to believe the individual would object,
- necessary to prevent or lessen a serious and imminent threat to someone's life or health, or
- permitted under the PPIP Act, Privacy Codes of Practice under the PPIP Act or the HRIP Act or other legislation.

The Council does not disclose sensitive personal information without consent, e.g., ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership, unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

5.2. Exemptions and the Privacy Code of Practice for Local Government

Exemptions to the Information Protection Principles (IPPs)

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

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

For example, s 23(3) of the PPIP Act provides that the 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.

Privacy Code of Practice for Local Government

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

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

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

For example, the Rates Record that the Council holds under s602 of the Local Government Act may be used to:
- notify neighbours of a proposed development,
- evaluate a road opening or
- evaluate a tree preservation order.

In addition, the Council may use personal information for other specific purposes where the Council is satisfied that the information is reasonably necessary for another function such as:
- understanding community and customer needs to improve our services,
- letting customers know about services or other information available (e.g., newsletters)
- sharing personal information within other divisions of the Council and authorised outsourced service providers to expedite services to customers.

5.3. Offences

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

5.4. The Health Records and Information Privacy Act

The HRIP Act sets out how the Council must manage health information. Health privacy principles Schedule 1 of the HRIP Act contains 15 Health Privacy Principles ('HPPs') that the Council must comply with.

The following is an overview of the principles as they apply to the Council.

Collection

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

Storage

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

Access and accuracy

The Council is transparent about the health information it holds, why it is used, and the right to access and amend it.
The Council allows people to access their own health information without unreasonable delay or expense.
The Council allows people to update, correct or amend their health information where necessary.
The Council ensures that health information is relevant and accurate before using it. Use
The Council only uses health information for the purpose it was collected for unless it has consent for its use for another purpose.

Disclosure

The Council does not disclose health information without consent, unless disclosure is permitted under the HRIPA or other legislation; Identifiers and anonymity 12. The Council may use unique identifiers for health information.
The Council allows people to remain anonymous where it is lawful and practicable. For example where possible our online surveys and other community engagement initiatives allow for feedback to be given anonymously.

Transfers and linkage

The Council does not transfer health information outside of NSW.
The Council does not currently use a health records linkage system.

5.5. Exemptions to the Health Privacy Principles (HPPs)

Exemptions are located mainly in Schedule 1 to the HRIP Act and may permit the Council not to comply with HPPs in certain situations.

For example, the Council is not required to comply with HPPs 4-8, and 10 if lawfully authorised or required not to do so.

5.6. Health Records and Information Privacy Code of Practice 2005

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

5.7. Offences

Offences can be found in s68-70 of the HRIP Act.

It is an offence for the Council to:
- intentionally disclose or use health information for an unauthorised purpose,
- offer to supply health information that has been disclosed unlawfully,
- Government.

6. Other Relevant Matters

6.1. ROLES AND RESPONSIBILITIES

The Information Officer and the Governance Coordinator will be responsible for the Policy and will coordinate the following functions in relation to the Policy:
- Maintaining appropriate records relating to the Privacy Management Plan and its application • Keeping the Plan current, and undertaking regular reviews of both the Plan and associated procedures
- Train and educate relevant employees with respect to the Plan and privacy in general and ensure documents, tools, templates and user guides are current and readily available.
- Provision of advice and ensuring adherence with the Plan and relevant legislation.

CEO
The CEO has the responsibility for appointing an appropriate officer as Council's Privacy Contact Officer to manage the day-to-day activities in relation to the appropriate collections, use and storage of personal and private information of customers and ratepayers

Divisional Managers
Divisional Managers are responsible for ensuring their Division adheres to the requirements of this Plan and provide guidance in respect of the importance of protecting the privacy and the personal information of customers and ratepayers collected and held by Council.

Divisional Managers should ensure that the privacy impacts of any new project or system development/implementation are thoroughly considered prior to implementation to allow issues of concern or risk to be addressed early in the process. Divisional Managers are to ensure that any adopted Privacy Impact Assessment process or procedure is followed whenever personal or health information will be collected, stored, used or disclosed in a project.

Staff
Staff shall adhere to the requirements of this Plan and be cognisant of the significant impact that can occur to individuals if their privacy is breached in any way or their personal information is not handled in accordance with this Plan and relevant legislation.

Staff should only access the personal information of a customer or ratepayer if it is a direct requirement of their role and should never release personal or private information to another person without prior approval by their supervisor. If any doubt exists in relation to any privacy

issue, including appropriateness of collecting, using or sharing personal and private information than staff should contact the Privacy Contact Officer immediately for direction.

6.2. Contracts with consultants and other private contractors

It is necessary to have specific provisions to protect the Council in any dealings with private contractors.

6.3. Confidentiality

The obligation of confidentiality is additional to and separate from that of privacy. Nevertheless, a duty to withhold information lies at the heart of both concepts. Confidentiality attaches to information per se, personal or health information to the person to whom that information relates.

An obligation of confidentiality exists for all employees whether express or implied as a matter of law.

Information which may be confidential is also likely to have a separate and independent obligation attaching to it in the form of privacy and in that regard, a release for the purposes of confidentiality will not suffice for privacy purposes. Two separate releases will be required and, in the case of privacy, the person to whom the information relates will be required to provide the release.

6.4. Misuse of personal or health information

Section 664 of the LG Act makes it an offence for anyone to disclose information except in accordance with that section. Whether or not a particular disclosure is made with lawful excuse is a matter that requires legal opinion from case to case.

6.5. Regular review of the collection, storage and use of personal or health information

The information practices relating to the collection, storage and use of personal or health information will be reviewed by the Council every three (3) years. Any new program initiatives will be incorporated into the review process with a view to ascertaining whether or not those programs comply with the PPIPA.

6.6. Policies, Legislation and Publications

The following legislation, policies and publications affect the processing of information related to this Plan:

***Privacy and Personal Information Protection Act 1998* (PPIPA)**

In addition to requirements covered in this plan, the PPIPA prohibits disclosure of personal information by public sector officers that are not done in accordance with the performance of their official duties. These provisions are generally directed at corrupt or irregular disclosure of personal information staff may have access to at work and not inadvertent failure to follow procedures or guidelines. Corrupt or irregular disclosure can include intentionally disclosing or using personal information normally accessed in staff undertaking their roles for an

unauthorised purpose, or to offer to supply personal information that has been disclosed unlawfully. Offences can be found listed in s62-68 of the PPIPA, are considered serious and may, in some cases, lead to imprisonment.

The PPIPA is available for viewing at www.ipc.nsw.gov.au

***Health Records and Information Privacy Act 2002* (HRIPA)**

The HRIPA governs both the public and private sector in NSW. It contains a set of 15 *Health Privacy Principles* and sets up a complaints mechanism to ensure agencies abide by them.

The HRIPA is available for viewing at www.ipc.nsw.gov.au

Council's *Public Access to Council Information Policy*

Public access to information and documents held by Council is facilitated by Council's *Public Access to Council Information Policy*. This Policy has regard to the *Government Information (Public Access) Act 2009* and the *Government Information (Public Access) Regulation 2009.*

This Plan should be read in conjunction with *the Public Access to Council Information Policy* held by Council, the *Privacy Code of Practice for Local Government*, together with Council's *Information Guide* and *Closed Circuit Television (CCTV) Policy.*

Council's Policy and Information Guide are available for viewing on Council's Website at www.shoalhaven.nsw.gov.au

The *Privacy Code of Practice for Local Government* can be obtained from the publications area of the Office of Local Government Website at www.olg.nsw.gov.au

***Public Interest Disclosures Act 1994* (PID Act)**

The definition of personal information under PPIPA excludes information contained in a public interest disclosure. This means that a person cannot seek review of the use or disclosure of a public interest disclosure or be prosecuted for unauthorised disclosure of public interest disclosure information under PPIPA. However, this plan is still able to address strategies for the protection of personal information disclosed under PID Act.

The PID Act is available for viewing at www.legislation.nsw.gov.au – further information can be obtained from the NSW Ombudsman at www.ombo.nsw.gov.au

6.7. Application Forms

Current application forms should be downloaded from Council's website at www.shoalhaven.nsw.gov.au. – See Quick Links – Forms for Download

6.8. Further information

For assistance in understanding the processes under the PPIPA and HRIPA, please contact the Council or the Office of the Privacy Commissioner NSW.

Council's policies and procedures comply with the PPIP Act and HRIP Act

Other legislation such as the Government Information (Public Access) Act 2009 and the Environmental Planning & Assessment Act 1979 requires Council to make certain documents available for public inspection. To the extent of any inconsistency, those requirements generally prevail over privacy legislation. Further details about public access to Council documents are contained in Council's Access to Information Policy, which is available on Council's website.

Council will ensure that any collection of personal information by use of security video cameras or other devices will be accompanied by appropriate signage as required by law. Council employees have been provided with notice regarding surveillance in accordance with the Workplace Surveillance Act 2005 and Council's Policy.

Information will be held in an appropriately secure manner. IT security requirements including the use of passwords are set out in Council's Acceptable Use of Communication Equipment Policy. Paper based and electronic records will be managed in accordance with Council's Records Management Policy. Information in documentary form is held and retained in accordance with the provisions of the State Records Act 1998. Any disposal of records is carried out in accordance with the approved disposal schedule: GDA 39 – General Retention and Disposal Authority for Local Government Records. Council will include in its documents concerning employment and in any contractual arrangements, provisions that ensure that staff, contractors and agents are aware of their obligations regarding the handling of personal or health information obtained in the course of their employment or engagement.

Council's Information and Privacy Officer and Council's Public Officer are the persons responsible for management of privacy related issues. This involves provision of information and advice regarding legislative obligations and the privacy implications of new projects, plans, initiatives or policies; dealing with inquiries from members of the public; managing or undertaking investigations of complaints; and review of Council policy, procedures and the Privacy Management Plan. The Privacy Management Plan is easily accessible on Council's website. Ongoing staff training will be provided on the management of personal and health information.

7. Privacy Contacts

Shoalhaven City Council
Information and Privacy Officer
PO Box 42
NOWRA NSW 2541

Telephone: (02) 4429 3111 or 1300 293 111
Email: council@shoalhaven.nsw.gov.au

Shoalhaven City Council
Public Officer
PO Box 42
NOWRA NSW 2541

Telephone: (02) 4429 3111 or 1300 293 111
Email: council@shoalhaven.nsw.gov.au

Information & Privacy Commission NSW
GPO Box 7011
SYDNEY NSW 2001

Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 472 679
Address: Level 1, McKell Building
2-24 Rawson Place
HAYMARKET NSW 2000

NSW Civil & Administrative Tribunal
PO Box K1026,
HAYMARKET NSW 1240

Phone: 1300 006 228
Email: aeod@ncat.nsw.gov.au
Address: Level 10, John Maddison Tower, 86-90 Goulburn Street, SYDNEY NSW 2000

8. Review period

This Plan will be reviewed every two years.