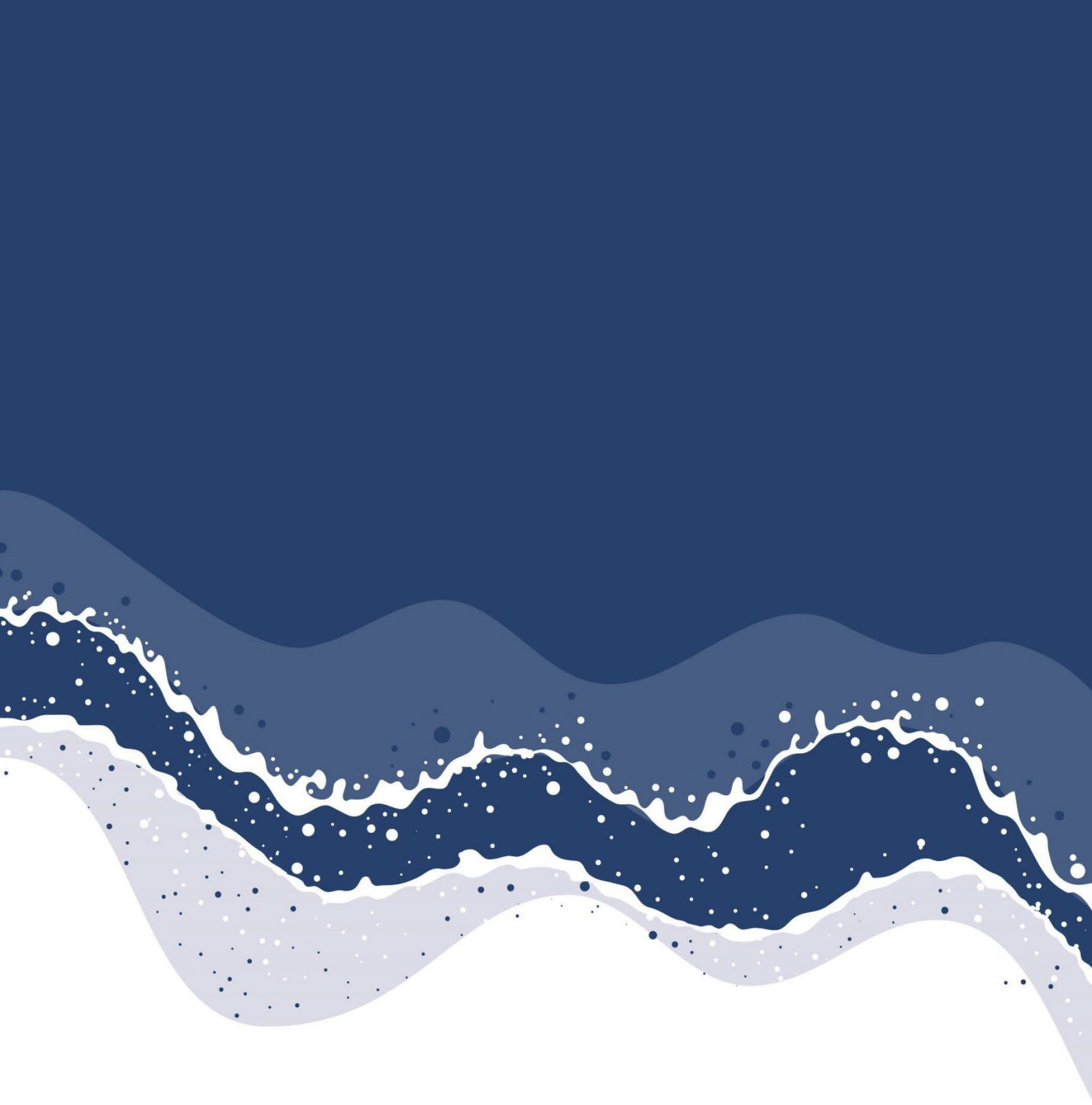

Privacy Policy

wyndhamcity
city. coast. country

Privacy Policy

Contents

Privacy Policy

PURPOSE

This policy establishes Wyndham City Council's overarching framework for the lawful, fair and transparent handling of personal information, including health information. It sets out the principles, requirements and responsibilities for the collection, use and disclosure, storage, correction, security, retention and disposal of that information in accordance with the *Privacy and Data Protection Act 2014* (Vic), including the Information Privacy Principles ('IPPs') and the *Health Records Act 2001* (Vic), including the Health Privacy Principles ('HPPs') (referred to collectively in this Policy as 'Personal Information'. Council's practices and related procedures, including privacy impact assessments (PIAs), privacy complaint and breach management procedures, or technology-specific or service-specific instruments must be consistent with this policy.

SCOPE

This policy applies to all Councillors, Council employees, agency personnel, volunteers, consultants, contractors, contracted service providers, suppliers, work experience students, placement participants, managed entities and their officers and staff and any other person who collects, accesses, uses, discloses, stores, manages or otherwise handles personal information for health information for or on behalf of Council.

POLICY STATEMENT

Council is committed to protecting privacy and to the lawful, transparent, responsible and fair handling of Personal Information.

As a Victorian local government authority, Council handles Personal Information under the Victorian statutory privacy framework, not as a Commonwealth agency under the Privacy Act 1988 (Cth), except to the extent any specific Commonwealth privacy obligation is expressly applicable.

Council will collect, use, disclose, store, secure, access, correct, retain and dispose of Personal Information in a way that respects the rights of individuals, supports public trust and is proportionate to Council's lawful functions and activities.

In doing so, Council will apply the requirements of applicable privacy legislation and will ensure that privacy considerations are embedded in decision-making, system design, service delivery, procurement, investigation, monitoring and governance activities.

Council also recognises its obligations as a public authority under the *Charter of Human Rights and Responsibilities Act 2006*, including the requirements to act compatibly with human rights when making decisions or taking actions.

POLICY OBJECTIVES

1. To establish Council's overarching framework for the lawful, fair, transparent and secure handling of Personal Information across Council's functions, services, systems and activities.

2. To explain at a policy level how Council collects, uses and discloses, stores, secures, provides access to, corrects, retains, de-identifies and lawfully disposes of Personal Information and how privacy complaints, enquiries and suspected privacy breaches are managed.

3. To ensure all Councillors and Council employees, agency personnel, volunteers, consultants, contractors, contracted service providers, suppliers, work experience students, placement participants, managed entities and their officers and staff and any other person who collects, accesses, uses, discloses, stores, manages or otherwise handles Personal Information for or on behalf of Council are aware of, and comply with, this policy and related privacy requirements.
4. To support consistent privacy governance across Council by providing the overarching privacy settings for related procedures, standards, privacy impact assessments, collection notices, contracts, systems and service specific or

technology specific instruments.

5. To promote a culture of privacy, accountability and privacy by design in Council's decision making, procurement, service delivery, monitoring, investigations and information management practices.

PRINCIPLES OR RULES

1. Collection of Personal Information

Council will only collect Personal Information where it is reasonably necessary for, or directly related to, Council's lawful functions, activities or services, and only by lawful and proportionate means. Where reasonable and practicable, Council will collect Personal Information directly from the individual concerned.

Council may also collect Personal Information indirectly where this is lawful and appropriate, including where direct collection is not reasonable or practicable, where the collection is required or authorised by law, or where information is incidentally captured as part of a lawful Council activity or system.

Where Personal Information is incidentally captured, Council will ensure that the collection remains connected to a legitimate Council purpose and is subject to appropriate safeguards, limitations and oversight.

This policy applies to all current and future Council practices, systems and technologies that collect, generate, infer, record or otherwise handle Personal Information.

This may include collection:

- directly from the individual;
- from an individuals authorised representative, guardian, legal adviser or health service provider;
- from contracted service providers, consultants or other organisations acting for or on behalf of Council;
- from publicly available sources where lawful and appropriate; through correspondence, telephone calls, applications, forms, meetings, complaints, requests, reports, surveys and consultations;
- through lawful monitoring, recording, safety, security, access-control or operational technologies;
- through surveillance or recording activities where an individual's image, voice, location, behaviour or other identifying information is intentionally or incidentally captured;
- where collection is required, authorised or otherwise permitted by law.

Monitoring and recording technologies

Council may use surveillance, monitoring and recording technologies where lawful and reasonably necessary to support its functions, activities and services, including safety, security, asset protection, compliance, investigation, regulatory or enforcement activities, service delivery, emergency management and other legitimate operational purposes.

This Policy applies to all such technologies, whether current or future, permanent or temporary, fixed or mobile, overt or otherwise lawfully deployed. Council will ensure that the use of such technologies is lawful, necessary, proportionate and supported by appropriate notice, governance, access controls, retention controls and review.

This includes, without limitation:

- permanent CCTV infrastructure, whether internal or external to infrastructure;
- temporary or deployable CCTV or surveillance units;
- mobile and vehicle mounted CCTV and surveillance systems;
- body worn cameras;
- security, access-control and entry-monitoring systems;

- sensors, intercoms and similar devices that capture or generate Personal Information;
- audio, visual, image-based, behavioural, access, location or metadata recording systems;
- any future technology used by Council for monitoring, recording, safety, security, compliance or operational purposes.

Children and young people

Council recognises that handling the Personal Information of children and young people requires additional care. Council will obtain the consent or authority from a parent, guardian or authorised representative, and handle this information in a manner that is lawful as well as child-safe, proportionate and appropriate to the child's age, maturity, capacity, service context and safety. In some circumstances, Council may deal directly with a child or young person where lawful, appropriate and consistent with their rights, wellbeing and safety.

This may include circumstances:

- involving youth services or programs;
- where the young person is capable of understanding the collection and use of their information;
- where obtaining parental involvement may not be appropriate, safe or practicable;
- where the law permits or requires Council to collect, use or disclose information without parental consent.

Sensitive or health related information

Council will not collect, use or disclose sensitive or health related information unless the individual has consented, or the collection, use or disclosure is otherwise required, authorised or permitted by law. Council will apply care, restrictions and safeguards when handling sensitive information and health information. Council will ensure that such information is only handled where it is genuinely necessary and relevant to the relevant function, activity or service.

This may include information:

- relating to physical or mental health, disability or care needs;
- connected to the delivery of maternal and child health, family, leisure, community, aged, youth or other services;
- relevant to employment, fitness for work, safety, injury management or contract administration;
- required for insurance claims or assessment, employment claims or complaints, investigations or regulatory compliance;
- required or authorised by law;
- necessary to prevent or lessen a serious and imminent threat to the life, health or safety of an individual or the public;
- necessary for the establishment, exercise or defence of a legal claim;
- necessary for research, compilation and analysis of statistics relevant to government funded community programs; or
- otherwise permitted by the Privacy Laws.

Confidential information

Information given in confidence to Council, including in its capacity as a health service provider, is handled in accordance with its legal obligations and the Privacy Laws.

Collection notices

Where Council collects Personal Information, it will take reasonable steps to provide an appropriate collection notice, unless an exception applies. Collection notices support transparency and help individuals understand why information is being collected, how it will be handled, and the consequences of not providing it, for example, it may mean that the provision of services by Council may be impacted.

Collection notices may be provided in a form appropriate to the circumstance and method of collection.

This may include collection notices provided:

- verbally, such as during phone calls or in-person interactions
- in writing on forms, applications, agreements, correspondence or notices
- electronically through websites (such as Council's website), portals, digital services or online forms
- by layered notice, where summary information is provided upfront and fuller information is available elsewhere
- by signage or other prominent notice where surveillance, recording or event-based collection is occurring.

A collection notice may explain:

- the purpose of collection;
- the legal authority or basis for collection, where relevant;
- the usual uses and disclosures of the information;
- whether provision of the information is required or optional;
- the consequences of not providing the information;
- how the individual may later seek access to or correction of the information.

Council routinely collects the following types of personal information:

- name, address, property, bank account and other financial details of residents and ratepayers for undertaking its rating and valuation services, town planning and building statutory functions and other property related services or the provision of Council services where these details are required;
- name, address and contact details of individuals who contact Council with respect to requests or complaints related to Council services, and those of individuals who are the subject of complaints, investigations and/or enforcement action;
- photographs, video, audio and other recordings taken in and about Council assets, premises, facilities, operations, meetings, events and public places, including for operational evidentiary, safety, security, service deliver, publicity, engagement and record keeping purposes;
- images and recordings of individuals and other data obtained from or about individuals through monitoring systems, recording, safety, security, access-control, fleet, compliance, enforcement or other operational technologies used by Council, whether fixed, mobile, temporary, permanent, vehicle-mounted, wearable, sensor-based, networked, automated or otherwise, including any future technologies of a similar nature implemented by Council for lawful Council purposes;
- age, occupation, physical disabilities, health related and other sensitive information of individuals receiving Council services related to childcare, maternal and child health, pre-school, youth, family, leisure and aged care;
- personal and sensitive information of (prospective and current) employees, consultants and contracted service providers relevant to their employment or contract with Council;
- name, address, bank account and other financial details of employees, including tax file number information which is governed by the Privacy Act 1988 (Cth);
- via Council's website and social media activities (e.g. Facebook) and other digital and online forums and websites which are used by Council to connect with the community and residents, to respond to inquiries, to promote Council events and services, and engage in community consultation and receive feedback. Some of these forums are public facing and Council uses commentary and content for various purposes including service improvement, staff training and in its publications.

2. Use and Disclosure

Council uses and discloses Personal Information for the primary purpose for which it was collected, for related purposes an individual would reasonably expect, or where otherwise required, authorised or permitted by law.

Council will not use or disclose Personal Information in a way that is unrelated, unnecessary or inconsistent with the purpose for which it was collected, unless a lawful basis exists to do so.

Where Personal Information is obtained through Council's operational, safety, security, surveillance, monitoring, recording or similar systems, authorised Council officers may access, use and disclose that Personal Information for the lawful management, optimisation, protection and administration of its services, assets, workforce and operations, provided that the access, use or disclosure is proportionate, relevant, reasonably necessary for a legitimate Council purpose, and subject to appropriate governance, approval, audit and access controls.

This may include primary purposes connected with the operation, safety, maintenance, utilisation, planning, allocation, coordination, protection and optimisation of Council services, assets and resources. It may also include secondary purposes where relevant to a specific complaint, incident, compliance, safety or performance matter, and where handled in accordance with Council's governance requirements and any applicable subordinate policy, procedure or approval process.

Where reasonable and practicable, Council will use de-identified Personal Information for analysis, research, planning, reporting or service improvement purposes.

This may include use or disclosure for:

- the provision, administration and improvement of Council services;
- rating, valuation, planning, building, local laws, animal management, waste, asset, community or regulatory functions;
- customer service, complaints handling, requests, investigations and enforcement activities;
- employment, recruitment and engagement, payroll, workplace management, procurement and contract administration;
- service delivery by contractors or service providers acting for or on behalf of Council;
- compliance with legislative, regulatory, reporting or audit obligations;
- emergency management, law enforcement or safety-related purposes;
- child information sharing, family violence information sharing, or other lawful information sharing arrangements;
- legal advice, legal proceedings, insurance, debt recovery, financial management or professional advisory services;
- service planning, community consultation, data analysis, quality assurance, training or improvement activities;
- operational planning, work allocation, asset utilisation, maintenance planning, service optimisation, productivity improvement and the efficient deployment of Council resources;
- the identification, assessment and management of operational, safety, security, conduct or compliance issues;
- the investigation of complaints, incidents, misconduct or suspected breaches of Council policy, procedure, contractual obligations or lawful directions;
- coaching, development, workplace management, complaint handling, investigation and disciplinary processes, where relevant to a specific operational, conduct, safety, compliance or performance matter and handled in accordance with Council's governance requirements.

Personal Information may be disclosed to (but not limited to) the following:

- a Council committee or committee meeting;
- Council's contracted service providers who manage the services provided by Council, including garbage collection, leisure centres, pre-schools, environmental health inspections and Infrastructure maintenance;
- statutory bodies (eg VicRoads, AGL) for purposes such as targeted consultation processes on projects that could affect residents;
- Greater Western Water for the purposes of ensuring that data held by both is maintained as correct and up-to-date as possible;
- an external regulator or authority in connection with the investigation of complaints or alleged unlawful

activity;

- individuals for the purpose of serving a notice to fence as required by the Fences Act 1968 (Vic) or a Protection Notice under the Building Act 1993 (Vic) or similar statutory requirements;
- Victorian Electoral Commission and Australian Electoral Commission for compilation of Voters Rolls;
- statutory bodies (e.g. Centrelink, Child Support Agency, Department of Families, Fairness and Housing, Department of Health, Department of Education, Transport Accident Commission, WorkCover and Australian Taxation Office) for purposes required or authorised by relevant legislation;
- Police, Fire department, SES or other body for emergency or law enforcement purposes;
- public registers that need to be maintained in accordance with other Acts, such as the planning register, building register, swimming pools and spa register, and domestic animals register;
- an individual's authorised representative, health service provider, legal adviser or superannuation fund;
- Council's consultants and professional advisers, including accountants, auditors, insurers, bankers, valuers, debt collection agents, IT providers and lawyers;
- organisations assisting Council to perform statistical analyses for improving the services being delivered to the community, noting that where practicable and reasonable, steps will be taken to de-identify the information in these circumstances;
- referees in connection with an employment application process;
- an agency or organisation to verify an individual's identity;
- an immediate family member of an individual, for emergency reasons or if it is necessary to provide the appropriate care or health service to the individual;
- housing support agencies to assist in the finding of alternative accommodation in cases of emergency;
- in building permits and plans to property owners and the Victorian Building Authority;
- the Lost Dogs Home, RSPCA and Australian Animal Registry for animal management purposes; and
- as authorised or required by law including under the Child Information Sharing Scheme established by the Child Wellbeing and Safety Act 2005 (Vic) and the Family Violence Information Sharing Scheme created by Part 5A of the Family Violence Protection Act 2008 (Vic).

Council will not disclose sensitive or health related information unless the individual has consented, or the disclosure is:

- required or authorised by law;
- necessary to prevent or lessen a serious and imminent threat to the life, health or safety of an individual or the public;
- necessary for the establishment, exercise or defence of a legal claim;
- necessary for research, compilation and analysis of statistics relevant to government funded community programs; or
- otherwise permitted by the Privacy Laws.

Automated systems, analytics and artificial intelligence

Council may use approved automated systems, analytics and artificial intelligence-enabled tools where lawful and appropriate to support service delivery, administration, analysis, operational efficiency and other legitimate Council purposes.

Where these tools involve Personal Information, Council will ensure appropriate governance, privacy assessment, security controls, human oversight and compliance with this Policy and any related Council policies, standards or procedures. Council will not use such tools in a manner inconsistent with the Privacy Laws.

This may include approved systems used for:

- Customer interactions and service support;
- Administrative workflows and document processing;
- Analysis of operational, environmental or asset-related data;
- Safety, inspection, maintenance or service optimisation activities;

- Reporting, planning, forecasting or performance monitoring.

As set out in Council's Artificial Intelligence Policy, Council is committed to maintaining transparency regarding its use of AI technologies, involving stakeholders in discussions about AI use, and conducting awareness campaigns about the use of AI. Only AI tools approved by Council may be used by Council staff and all AI use must adhere to strict data privacy protocols.

3. Data Quality, Confidentiality and Security

Personal Information collected by Council is stored securely in both physical and electronic formats. Council uses cloud-based and on-premises systems that are protected by multi-layered cybersecurity measures. Where cloud services are provided by third parties, Council ensures that service providers maintain equivalent levels of privacy and security protection, consistent with Privacy Laws. Council therefore maintains secure systems for storing Personal Information and utilises appropriate technologies, security methods, operational policies and procedures to protect the Personal Information from unauthorised access, improper use, alteration, unlawful or accidental destruction and accidental loss.

Council takes reasonable steps to ensure that Personal Information that it collects, uses or discloses is accurate, complete and up to date.

Council conducts data matching periodically to ensure accurate name records are maintained on individual customers.

4. Access and Correction

Individuals are encouraged to contact Council to request changes to their contact details so that Council records are up to date.

Individuals may request access to, deletion or correction of, their personal information in accordance with the Privacy and Data Protection Act 2014 (Vic). Requests are usually managed under the Freedom of Information Act 1982 (Vic) and are subject to the requirements of the Public Records Act (Vic) 1973.

Please contact the Privacy Officer in the first instance to discuss your requirements via **privacy@wyndham.vic.gov.au**.

5. Unique Identifiers and Anonymity

Whenever it is lawful and practicable, individuals have the option of transacting with Council anonymously and not identifying themselves. Customers can make a complaint anonymously. However, in some cases, Council's response may be limited in these circumstances. For example, it may not be possible to investigate an anonymous complaint without making inquiries and obtaining further information.

Council maintains a central 'Name and Address Register' (NAR database) and assigns a unique NAR identifier to each individual to ensure that there is only one name record for each individual customer so as to maintain data integrity. The NAR database may be used by Council to contact residents, ratepayers and customers in relation to Council functions and services.

6. Transborder Data Flows

Council may transfer Personal Information to an individual or organisation outside Victoria but only in limited circumstances:

- where the individual has consented;
- if the recipient of the information is subject to a law, binding scheme or contract which is substantially similar to the Privacy Laws; or
- where otherwise permitted under the Privacy Laws.

Council takes all reasonable steps to ensure that contractors and cloud service providers in accordance with the IPP's and HPP's.

7. Privacy Breaches

Staff and contractors are required to notify their supervisor on becoming aware of an actual or suspected breach of the IPP's or HPP's by Council. Supervisors must inform the Privacy Officer of actual breaches. The Privacy Officer is responsible for ensuring that the breach is addressed and managed in accordance with the IPP's or HPP's (as relevant) and Council's Privacy Complaints and Breach Management Procedure.

8. Complaints or Enquiries

Any person who is concerned about Council's management of their Personal Information or believes that their privacy has been breached may submit an inquiry or make a complaint to Council's Privacy Officer via privacy@wyndham.vic.gov.au. The Privacy Officer will address the complaint in accordance with the Privacy Complaints and Breach Management Procedure.

Alternatively, a complaint may be directed to the Office of the Victorian Information Commissioner (OVIC) with respect to personal information, or the Office of the Health Complaints Commissioner for health information, including if a person is dissatisfied with Council's handling of their complaint.

Please note that the respective Commissioners may decline to entertain the complaint, if a complaint has not been first raised with Council.

ROLE ACCOUNTABILITIES & RESPONSIBILITIES	
Council / Chief Executive Officer	• Provide leadership and ensure appropriate governance, systems, resources and culture are in place to support privacy compliance across Council. • Endorse and support implementation of the Privacy Policy and related privacy governance arrangements. • Ensure significant privacy risks, serious privacy incidents and systemic privacy issues are addressed appropriately through Council's governance framework
Director Corporate Services	• Has executive oversight of privacy management at Council • Is a Council Privacy Officer • Ensures privacy governance is appropriately supported across corporate and operational functions.
General Counsel	• Policy owner. • Provides legal advice and guidance on privacy, confidentiality, information sharing, surveillance, compliance and related legislative matters. • Supports interpretation, review and continuous improvement of the Privacy Policy and related instruments.
Team Leader FOI & Privacy; Senior FOI and Privacy Officers	• Act as Council's Privacy Officers • Receive and respond to privacy complaints and enquiries • Coordinate and oversee response to actual or suspected privacy breaches and privacy incidents • Advise on privacy clauses in contracts, collection notices, privacy statements and related controls • Review and sign off on Privacy Impact Assessments • Regularly review this Privacy Policy, associated procedures and the Website Privacy Statement • Develop, maintain and deliver privacy guidance and training materials

Manager IT Services, Co-ordinator Operations IT Services	• Responsible for Council's compliance with the Victorian Protective Data Security Framework and Standards • Implement and maintain information security controls for systems that collect, store, process or transmit personal information and health information • Support privacy breach and information security incident response, including containment, technical investigation and remediation • Support secure system design, access control, auditability, retention and monitoring capabilities for privacy-relevant systems
Directors, Department Managers and Team Leaders	• Promote and ensure privacy compliance within their business areas • Ensure staff complete required privacy training and understand applicable privacy, confidentiality, records and security obligations • Foster a culture of responsible information management and privacy by design • Identify privacy risks in business processes, projects, technologies and service delivery and implement appropriate controls in consultation with Council's Privacy Officers • Ensure privacy complaints, incidents and suspected breaches are escalated appropriately
Project Sponsors, Business Owners and System Owners	• Ensure privacy requirements are considered at the earliest stage of projects, procurements, initiatives, system changes and new technologies. • Ensure a Privacy Impact Assessment is undertaken for new projects, initiatives, systems or material changes involving personal information or health information, in consultation with Council's Privacy Officers. • Implement and maintain approved privacy controls, notices, settings, access arrangements and risk treatments. • Ensure personal information handling remains consistent with the approved purpose, legal basis and governance controls for the project or system.
Procurement Contract Managers and Contract Owners	• Ensure contracts and third-party arrangements include appropriate privacy, confidentiality, security, access, audit, breach notification, retention and disposal requirements. • Ensure consultants, contractors and service providers handling information on Council's behalf understand and comply with applicable privacy obligations. • Monitor privacy-related obligations throughout the life of the contract or engagement.
Records and Information Management and FOI functions	• Support compliance with records management, retention, archival and lawful disposal requirements for records containing personal information and health information. • Support alignment between privacy, FOI and public records obligations. • Support document accessibility and record retrieval where required under lawful processes
People and Capability	• Support privacy induction, training and awareness activities relevant to employees and workplace processes. • Support the management of privacy issues arising in employment, conduct, workplace management and personnel matters, in consultation with Privacy Officers and relevant leaders. • Where required under subordinate policies or procedures, support approval or governance processes relating to access to workforce-related monitoring data.

All Councillors, staff, agency personnel, volunteers, contractors, consultants, placement participants, and any other person handling information for or on behalf of Council	• Comply with this Policy and applicable privacy, confidentiality, records and security requirements. • Handle personal information and health information lawfully, fairly and only for authorised Council purposes. • Complete required privacy training and follow lawful and reasonable directions relating to privacy and information handling. • Promptly report actual or suspected privacy complaints, incidents or breaches through Council's reporting channels. • Refer privacy complaints, statutory requests for personal information, and suspected breaches to Council's Privacy Officers.

DEFINITIONS

For the purposes of this Privacy Policy, personal information includes sensitive information and health information unless the context indicates otherwise.

Artificial Intelligence (AI) – means the simulation of human intelligence in machines that are programmed to think and learn like humans. AI encompasses a wide range of technologies and techniques that enable machines to perform tasks that typically require human intelligence, including problem-solving, learning, planning, speech recognition, natural language understanding, perception, and decision-making.

Council – means Wyndham City Council, including all Councillors, Council staff, consultants and contracted service providers, volunteers and students.

Health information means information or opinion about the physical, mental, psychological health of an individual, disability of an individual or a health service provided or to be provided to an individual but does not include information about an individual who has been deceased for more than 30 years.

Personal information – as defined by the Privacy Laws, means information or opinion, whether true or not and whether recorded in material form or not, about a living individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

Privacy Laws means the *Privacy and Data Protection Act 2014* (Vic) and the *Health Records Act 2001* (Vic) and in some cases the *Privacy Act 1988* (Cth).

Sensitive Information means information or opinion about an individual's ethnic origins, religious beliefs, political opinions or association, philosophical beliefs, membership of professional association or trade union, sexual orientation or practices and criminal record.

BREACH OF POLICY

Our staff are bound to act in line with Council's Code of Conduct and in compliance with the law. Under the Local Government Act, staff are required to perform their duties in accordance with Council values and meet the obligations of their roles, as communicated in Council's policies. Contravention of policy may constitute misconduct and result in disciplinary outcomes, including termination of employment.

REFERENCES

Legislative requirements:

- *Child Wellbeing and Safety Act 2005*
- *Child Wellbeing and Safety (Information Sharing) Regulations 2018*
- *Family Violence Protection Act 2008*
- *Family Violence Protection (Information Sharing and Risk Management) Regulations 2018*
- *Freedom of Information Act 1982*
- *Local Government Act 1989*
- *Health Records Act 2001*
- *Local Government Act 2020*
- *Local Government (Governance and Integrity) Regulations 2020*
- *Privacy Act 1988 (Cth)*
- *Privacy and Data Protection Act 2014*
- *Public Records Act 1973*
- *Victorian Data Sharing Act 2017*

Policies and Procedures:

- *Public Transparency Policy*
- *Records and Information Disposal Policy*
- *Information Security Policy*
- *CCTV Operational Policy*
- *AI Policy*
- *Privacy Complaints and Breach Management Procedure*
- *Privacy Impact Assessment Procedure*

VERSION HISTORY				
ID	**DATE**	**AUTHOR**	**REVISION REASON / KEY CHANGES**	**REVIEW DATE**
A1611318	21 March 2017	Wyndham Council Privacy Policy	Expired 21/03/2021	February 2028
8914378	23 June 2026	Wyndham Council Privacy Policy 2026		June 2027

DOCUMENT CONTROL	
DOCUMENT NAME	Privacy Policy – Legal Services
DOCUMENT ID	8914378 v2
OWNER	Legal Services - Privacy
ENDORSED	23 June 2026