Privacy and Health Information Policy

Policy outcome	The City of Port Phillip protects the privacy of individuals by responsibly and transparently managing personal and health information in accordance with Victorian privacy legislation.
Responsible division	Governance and Performance
Responsible department	Governance and Advocacy
Policy owner	Alli Griffin, Senior Privacy and FOI Advisor
Final approver	Executive Leadership Team (ELT)
Version	3
Date approved / adopted	13/04/2026
Planned review date	13/04/2030 *Every four years from approval date with a desktop review every two years*
Type of review	Refresh
Supersedes	Information Privacy Policy 2019 and Health Records Policy 2018

Document History

Version	Date	Review type	Changes made	Approved by
3.0	13/4/2026	New Instrument	New combined Policy replacing Information Privacy Policy 2019 and Health Records Policy 2018	ELT

Table of Contents

1. Purpose

This Policy provides a framework for the City of Port Phillip (Council) to ensure the lawful and appropriate collection, storage, use, disclosure, and management of personal information and health information in accordance with the *Privacy and Data Protection Act 2014 (Vic)* and the *Health Records Act 2001 (Vic)*.

This Policy demonstrates Council's commitment to:

- Maintaining the responsible and transparent handling of personal and health information
- Promoting education and awareness of privacy practices across the organisation
- Recognising the heightened sensitivity of health information and ensuring appropriate protections
- Providing individuals with rights of access to information about themselves held by Council
- Providing individuals with the right to request corrections to their personal information

Ten Information Privacy Principles (**IPPs**) underpin the *Privacy and Data Protection Act 2014 (Vic)* and 11 Health Privacy Principles (**HPPs**) underpin the *Health Records Act 2001 (Vic)*. IPP 5 and HPP 5 specify that organisations must have a written policy outlining how they manage personal and health information and that it must be provided to anyone who requests it.

2. Scope

This Policy applies to:

- All Councillors
- All Council officers (employees)
- Agents (consultants, agency staff, contractors those on work experience, and volunteers)
- Contracted service providers

This Policy applies when these persons are acting in the capacity for which they have been engaged or elected to Council and when representing the organisation in an official or unofficial capacity.

This Policy covers all personal and health information about an individual that is collected, stored, used, or disclosed by Council:

- in person
- over the telephone
- as correspondence or on forms (both paper and electronic)
- through Council's social media platforms and websites
- through CCTV and surveillance systems
- through artificial intelligence tools and systems.

This Policy encompasses Council's role as both a Local Government authority and as an employer, including the management of staff records and employee personal information.

3. Legislative Context

Council recognises that in meeting its statutory obligations, it must balance public interest in the free flow of information with an individual's right to privacy and the protection of personal, health, and sensitive information.

3.1 Information Privacy Principles (*Privacy and Data Protection Act 2014*)

Section 13(1)(c) of the *Privacy and Data Protection Act 2014 (Vic)* applies to Councils in Victoria. Schedule 1 of this Act outlines ten Information Privacy Principles that apply to Council:

- IPP 1 - Collection
- IPP 2 - Use and Disclosure
- IPP 3 - Data Quality
- IPP 4 - Data Security
- IPP 5 - Openness
- IPP 6 - Access and Correction
- IPP 7 - Unique Identifiers
- IPP 8 - Anonymity
- IPP 9 - Transborder Data Flows
- IPP 10 - Sensitive Information

A summary of the IPPs is provided in Attachment 1.

3.2 Health Privacy Principles (*Health Records Act 2001*)

The *Health Records Act 2001 (Vic)* contains 11 Health Privacy Principles that regulate the handling of health information. Health information is afforded additional protections recognising its sensitive nature and the potential for greater harm if mishandled.

- HPP 1 - Collection
- HPP 2 - Use and Disclosure
- HPP 3 - Data Quality
- HPP 4 - Data Security and Retention
- HPP 5 - Openness
- HPP 6 - Access and Correction
- HPP 7 - Identifiers
- HPP 8 - Anonymity
- HPP 9 - Transborder Data Flows
- HPP 10 - Transfer or Closure of the Practice of a Health Service Provider
- HPP 11 - Making Information Available to Another Health Service Provider

A summary of the HPPs is provided in Attachment 2.

4. Policy

4.1 Statement of Commitment

The City of Port Phillip is committed to protecting the privacy of personal and health information it collects and manages by complying with its obligations under the *Privacy and Data Protection Act 2014 (Vic)* and the *Health Records Act 2001 (Vic)*.

Council recognises that protecting individuals' personal and health information is essential to maintaining community trust and is a fundamental element of good governance, accountability, and integrity across all Council services, programs, and operations.

4.2 Collection of Personal and Health Information (IPP 1 / HPP 1)

Council will only collect personal or health information that is necessary for one or more of Council's functions or activities. Council will collect information only by lawful and fair means, and not in an unreasonably intrusive way.

If it is reasonable and practicable to do so, Council will collect personal or health information only from the individual concerned. If Council collects personal information about an individual from someone else, Council will take reasonable steps to ensure that the individual is made aware of the matters listed in Section 4.2.1, except where doing so would pose a serious threat to the life or health of any individual.

Council collects personal information for purposes including but not limited to:

- providing requested services (e.g., parking compliance, waste services, community services)
- processing applications (e.g., planning permits, building permits, animal registration)
- collecting Council fees and charges (e.g., rates notices)
- responding to enquiries and complaints
- enabling payment for goods and services
- supporting Council's law enforcement functions
- distributing information about Council initiatives and programs
- conducting surveys and community engagement
- administering health services (e.g., maternal and child health, immunisation) – this includes the collection of health information necessary to deliver immunisation services in accordance with applicable public health and immunisation frameworks.
- employment and recruitment purposes.

Where Council collects health information, it will only do so if:

- the individual has provided consent; or
- the collection is required, authorised, or permitted by or under law; or
- the collection is necessary to provide a health service and the individual is incapable of giving consent; or

- the collection is necessary to prevent or lessen a serious threat to life, health, safety, or welfare; or
- the collection is necessary for research or statistical analysis in the public interest and conducted in accordance with the Health Complaints Commissioner guidelines.

4.2.1 Children and parental information

Council health services, including Maternal and Child Health services, may collect personal and health information about children, parents or carers, and relevant family or household context. Where services are provided to children, consent for the collection, use and disclosure of information is obtained from a parent or person with parental responsibility, in accordance with law, professional standards and this Policy.

4.2.2 Privacy Collection Notices

At or before the time of collection (or as soon as practicable after), Council will take reasonable steps to ensure that individuals are aware of:

a) The identity of Council and how to contact it.
b) The purpose(s) for which the information is being collected.
c) Who your information may be shared with, such as service contractors or government authorities.
d) Any law that requires the particular information to be collected.
e) The main consequences (if any) for the individual if all or part of the information is not provided.
f) The fact that they can seek access to the information.

Privacy collection notices may be provided in the form of a written notice on forms, a notice in an automated telephone message, online webfoms, text on a webpage, or signage at the point of collection.

4.3 Use and Disclosure (IPP 2 / HPP 2)

Council will use personal or health information for the primary purpose for which it was collected, or for a related secondary purpose that the individual would reasonably expect.

Council will not use or disclose information about an individual for a secondary purpose unless one of the following applies:

- The secondary purpose is directly related to the primary purpose, and the individual would reasonably expect Council to use or disclose their information for that purpose.
- The individual has consented to the use or disclosure.
- The use or disclosure is required, authorised, or permitted by or under law.
- Council reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare, or a serious threat to public health, public safety, or public welfare.

- Council has reason to suspect unlawful activity and uses or discloses the information as a necessary part of its investigation or in reporting concerns to relevant authorities.
- Council reasonably believes the use or disclosure is reasonably necessary for law enforcement purposes.
- The use or disclosure is necessary for research or statistical analysis in the public interest (where it is impracticable to seek consent and the information will not be published in identifiable form).
- The individual is incapable of giving consent (as defined in the *Health Records Act 2001 (Vic)*.

4.3.1 Information sharing and safety frameworks

Nothing in this Policy limits or overrides Council's obligations under the Child Information Sharing Scheme (CISS), Family Violence Information Sharing Scheme (FVISS), mandatory reporting laws, or the Multi-Agency Risk Assessment and Management.(MARAM) framework. Where information sharing is required or authorised under these schemes, it is permitted for the purposes of IPP 2 and HPP 2.

When authorised or required by law, Council may disclose personal information to:

- government departments and agencies (including the Department of Families, Fairness and Housing, Department of Health, Victorian Workcover Authority, Department of Transport and Planning)
- law enforcement agencies, including courts and Victoria Police
- legal advisors and insurance providers
- relevant authorities and parties for workplace incident reporting, occupational health and safety compliance, injury management and workers' compensation claims
- contracted service providers acting on Council's behalf
- debt collection agencies
- road Traffic Authorities (for processing infringement notices)
- other organisations where disclosure is necessary to lessen or prevent a serious threat
- ASIO or ASIS where requested in connection with their functions.

Where disclosure is for law enforcement purposes, Council will make a written record of the disclosure.

Personal information may be disclosed to contracted service providers where it is necessary for the contractor to carry out a task on Council's behalf. All contracted service providers handling personal information are required to comply with the *Privacy and Data Protection Act 2014 (Vic)* and the *Health Records Act 2001 (Vic)* as a mandatory requirement of any contract.

4.3.2 Disclosure of Health Information

Health information is subject to additional protections. Council may use or disclose health information without consent only in limited circumstances, including:

- Where Council is providing a health service and the use or disclosure is reasonably necessary for provision of that service, and the individual is incapable of providing consent.
- Where the health information is used for the purpose of providing further health services to the individual safely and effectively.
- For the purpose of funding, management, planning, monitoring, improvement or evaluation of health services, or training provided to staff (where reasonable steps are taken to de-identify the information and it is not published in identifiable form).
- Where the use or disclosure of health information is required or authorised by law, including for public health and immunisation reporting obligations, such as the administration, monitoring, evaluation and oversight of immunisation programs.
- Where disclosure is necessary to lessen or prevent a serious threat to life, health, safety or welfare.
- To an immediate family member where necessary to provide appropriate health services or care to the individual, or for compassionate reasons, and the individual is incapable of giving consent and the disclosure is not contrary to any wish previously expressed by the individual.
- In child-centred health services, disclosure to immediate family members will generally only occur where appropriate to the clinical context or at the request of the parent or legal guardian, and in accordance with professional guidelines.

Council will make health information available to another health service provider where requested by the individual, their authorised agent, or where required by law.

4.3.3 Planning Applications

To meet our transparency obligations while complying with the *Planning and Environment Act 1987 (Vic)* and privacy legislation, Council will:

- inform applicants and submitters at the time personal information is collected that certain information must be disclosed or made publicly available as part of the statutory planning process.
- explain how personal information will be handled, including:
    - what planning documents or information may be made available for public inspection.
    - what information may be shared with referral authorities or other government bodies as required for assessment; and
    - what personal information will be retained for internal Council purposes only.
- limit public disclosure to what is required by law, ensuring that only necessary information is made publicly available, such as the address of the subject land, and that personal information is not published unless required or authorised by legislation.

- apply redaction and privacy-protective practices wherever possible and appropriate, to minimise unnecessary exposure of personal information in publicly accessible planning documents.
- direct individuals to relevant legislative requirements, so they understand the statutory basis for the collection, use and disclosure of personal information in the planning application process.

4.3.4 Public Submission (general)

When the community provides submissions, whether for consultations, advisory committees, or general engagement, Council will:

- provide a clear collection notice at the point of collection, explaining why information is being collected and how it will be used, shared, or published
- inform contributors if their submissions (including names) may be published in Council reports, agendas, minutes, consultation summaries, or on Council's website
- ensure submitters know who will see their information, such as Councillors, staff working on the matter, or external consultants assisting with the engagement process
- only publish or share the minimum personal information necessary and avoid including contact details or sensitive information unless required
- where it is appropriate to do so, Council will remove or deidentify personal information from submissions before including them in publicly accessible documents, including Council reports and attachments.

4.3.5 Council and Committee Meetings (including livestreaming and records)

To ensure transparency while respecting privacy during public meetings, Council will:

- provide notice to anyone making a written submission that their name - and possibly the content of their submission - may be included in the publicly accessible agenda and minutes
- advise individuals speaking at public meetings that the meeting is livestreamed, recorded, and published online, meaning their voice and statements may be publicly accessible for an indefinite period
- ensure signage and verbal reminders are in place at the meeting venue to notify attendees of livestreaming and recording
- remove unnecessary personal information from published materials unless required for transparency or compliance with legislation
- direct individuals to Council's Live Streaming Policy for full details of how recordings are managed.

- remind all attendees, including Councillors, Council officers, and community members to avoid disclosing personal or sensitive information about others during meetings unless required by law or necessary for the matter being discussed.

4.4 Data Quality (IPP 3 / HPP 3)

Council will take reasonable steps to ensure that all personal and health information collected, used, or disclosed is accurate, complete, up-to-date, and relevant to Council's functions or activities.

Council will systematically update any new personal information provided to existing records to ensure records are complete and current.

Individuals may request the correction of any personal or health information they have provided to Council, in line with Council's obligations under IPP 6 and HPP 6 (refer to section 4.7).

4.5 Data Security and Retention (IPP 4 / HPP 4)

Council will take all reasonable measures to protect personal and health information from misuse, loss, and from unauthorised access, modification, or disclosure.

Council employs a range of safeguards including:

- Procedural safeguards (policies, procedures, training).
- Physical safeguards (secure storage, access controls, clean desk practices).
- Technical safeguards implemented in accordance with Council's information security and technology standards.
- Backup and disaster recovery systems.

All records containing personal and health information will be managed in accordance with mandatory standards established under the *Public Records Act 1973 (Vic)* and relevant Retention and Disposal Authorities issued by Public Record Office Victoria (PROV).

Council will destroy personal information when no longer required for any purpose, in accordance with applicable Retention and Disposal Authorities issued by PROV.

Council will permanently de-identify personal information on request where it is lawful and practicable to do so, in accordance with IPP 4.2.

A health service provider must not delete health information unless permitted by law, or the deletion occurs after the individual attains the age of 25 years (for information collected when they were a child) or more than seven years after the last occasion on which a health service was provided, whichever is later. Where health information is deleted, Council will make a written note of the name of the individual, the period covered, and the date of deletion.

4.6 Openness (IPP 5 / HPP 5)

This Policy sets out Council's approach to managing personal and health information. A copy of this Policy is available on:

- Council's website www.portphillip.vic.gov.au
- At Council offices
- Or by calling 9209 6777 or emailing helpprivacy@portphillip.vic.gov.au

On request, Council will take reasonable steps to let an individual know:

- Whether Council holds personal or health information about them.
- What type of information is held and the nature of that information.
- The purpose for which the information is used.
- How Council collects, holds, uses, and discloses that information.
- The steps the individual should take to access their information.

4.7 Access and Correction (IPP 6 / HPP 6)

Individuals have a right to request access to personal or health information Council holds about them. If an individual believes their information is inaccurate, incomplete, misleading, or out of date, they may request Council to correct it.

Council may deny access in certain circumstances, including where:

- access would pose a serious threat to the life or health of any person
- access would have an unreasonable impact on the privacy of other individuals
- the request for access is frivolous or vexatious
- there are legal proceedings between the person and Council and the information would not be accessible by discovery
- providing access would reveal the intentions of Council in negotiations in a way that would prejudice those negotiations
- providing access would be unlawful or is prohibited by law
- providing access would be likely to prejudice an investigation of possible unlawful activity
- providing access would be likely to prejudice a law enforcement function
- a law enforcement agency requests that access not be provided on security grounds
- the request has been made unsuccessfully on a previous occasion and there are no reasonable grounds for making it again.

If Council refuses access, Council will provide written reasons for the refusal. Where access is refused on grounds that it would pose a serious threat to life or health, the individual may request that the information be made available to a health service provider nominated by them.

If an individual establishes that information is not accurate, complete, or up to date, Council will take reasonable steps to correct the information.

Council will respond to requests for access or correction as soon as practicable, but no later than 30 days after receiving the request.

Requests for access to records relating to children are generally managed under the *Freedom of Information Act 1982 (Vic).* Informal access is discretionary and limited to low-risk administrative

matters, and does not apply to requests for full records, health information, or where access is disputed or relies on parenting or court orders.

Requests for access to, or correction of, personal and health information are generally managed under the *Freedom of Information Act 1982 (Vic)*. However, requests can be dealt with informally outside this Act. Requests should be directed to Council's Privacy Officer in the first instance (see Section 9 for contact details).

4.8 Unique Identifiers (IPP 7 / HPP 7)

Council will only assign unique identifiers to individuals where necessary to enable Council to carry out its functions efficiently.

Council will not adopt unique identifiers assigned by other organisations (such as Medicare numbers, driver's licence numbers, or tax file numbers) as its own identifier unless:

- it is necessary for Council to fulfil its obligations to the other organisation
- one of the exceptions for use or disclosure under IPP 2.1(d) to (g) or HPP 2.2(c) to (l) applies
- the individual has provided consent
- the use or disclosure is required or authorised by law.

Council will not require an individual to provide a unique identifier assigned by another organisation to access a Council service unless provision is required or authorised by law, or is directly related to the purpose for which the identifier was originally assigned.

4.9 Anonymity (IPP 8 / HPP 8)

Where it is lawful and practicable, Council will give individuals the option of not identifying themselves when entering into transactions with Council.

However, in some situations it may not be lawful or practical for a person to remain anonymous, such as when:

- seeking health services
- lodging planning or building applications
- applying for permits or registrations
- making payments
- lodging complaints where identification is necessary to investigate or respond
- participating in Council or Committee meetings as a speaker, where individuals are generally required to identify themselves for the public record and transparency of proceedings.

Council will advise individuals of any limitations to services if personal information is not provided.

4.10 Transborder Data Flows (IPP 9 / HPP 9)

Council may transfer personal or health information outside Victoria only if:

- Council reasonably believes the recipient is subject to a law, binding scheme, or contract which effectively upholds principles for fair handling of the information that are substantially similar to the IPPs or HPPs.
- The individual consents to the transfer.
- The transfer is necessary for the performance of a contract between the individual and Council, or for implementation of pre-contractual measures taken in response to the individual's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between Council and a third party.
- The transfer is for the benefit of the individual, it is impractical to obtain consent, and the individual would likely consent if asked.
- Council has taken reasonable steps to ensure the information will not be held, used, or disclosed by the recipient inconsistently with the IPPs or HPPs.
- The transfer is required or authorised by law.

Council may use cloud computing services hosted outside Victoria. In such cases, Council will take reasonable steps to ensure information is protected consistently with Victorian privacy requirements through a Privacy Impact Assessment and contractual arrangements with the service provider that ensure equivalent protections.

4.11 Sensitive Information (IPP 10)

Council will not collect sensitive information unless one or more of the following applies:

- The individual has provided consent.
- The collection is required or authorised by or under law.
- The collection is necessary to prevent or lessen a serious threat to life or health, and the individual is unable to provide or communicate consent.
- The collection is necessary for the establishment, exercise, or defence of a legal or equitable claim.

Sensitive information includes information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, or criminal record.

Sensitive information will be treated with heightened security and confidentiality and only used for the purpose for which it was collected.

4.12 Transfer or Closure of Health Service Provider (HPP 10)

If a Council health service is to be transferred, amalgamated, or closed, Council will:

- publish a public notice on the Public notices - City of Port Phillip page stating that the service has been or is about to be transferred or closed

- state in the notice how Council proposes to deal with health information held about individuals who have received health services, including whether Council proposes to retain the information or make it available for transfer
- take any additional steps to notify individuals in accordance with the Health Complaints Commissioner guidelines.

Not earlier than 21 days after giving notice, Council will elect to either to:

- retain the health information; or
- transfer it to:

  The health service provider who takes over the service; or\The individual or a health service provider nominated by the individual.

If Council elects to retain health information, it must continue to hold it securely or transfer it to a competent organisation for safe storage in Victoria, until such time as the information may be destroyed in accordance with HPP 4.

4.13 Making Information Available to Another Health Service Provider (HPP 11)

If an individual requests Council to make their health information available to another health service provider, or authorises another provider to request the information on their behalf, Council will provide a copy or an accurate written summary of that health information as soon as practicable.

Council may charge a fee for providing this service, not exceeding the maximum amount prescribed in the Health Records Regulations 2023.

5. Council's Websites and Online Services

Council's website can be visited anonymously. Personal information is only collected when an individual:

- completes online forms (e.g., for payments, service requests, or applications)
- contacts Council through a website
- provides feedback via online surveys and forms
- subscribes to Council publications or mailing lists.

Council's website contains links to third-party websites and services. Information collected by third-party websites is managed in accordance with the third party's privacy policies. Council is not responsible for the privacy practices of third-party websites.

5.1 Cookies and Analytics

Council websites use cookies to help understand how people interact with Council services and to improve the user experience. Cookies do not collect identifying data and websites can be used if cookies are disabled.

For statistical and system administration purposes, Council websites may use analytics tools (such as Google Analytics) to collect non-personal information, including:

- Date and time of visit
- Pages accessed and downloaded
- Address of the previous website visited
- Type of browser used
- Type of device used
- Location (country, region, city)

This information is used solely to update and improve Council's websites.

Council will not attempt to identify any individual from this data unless it becomes necessary for investigating a potential breach of law or regulation.

5.2 Social Media

Council maintains social media accounts on platforms including Facebook, Instagram, X, LinkedIn and YouTube.

Council may collect information posted on social media for the purpose of engaging with and understanding the views of the community. Where individuals prefer not to communicate with Council via social media, alternative contact methods are available.

When a user logs in to a Council website using a social networking service account, Council may collect and store the unique user ID provided by that service. This user ID is used solely to identify the individual and enable access to specific website features. Council does not access or collect additional information from the user's social media profile, and the user ID is kept confidential.

6. Phone Call Recording

Notice and purpose
At the commencement of external calls to Council's Customer Service Centre, callers are advised that the call may be recorded for training, service improvement, and quality assurance purposes. This announcement functions as a collection notice, as required under the *Privacy and Data Protection Act 2014 (Vic)*.

Caller choice (consent/optout)
If a caller does not wish their call to be recorded, they should advise the attending officer at the beginning of the call. Upon request, the officer will stop the recording or offer an alternative communication channel, such as a nonrecorded call, an in-person appointment, or a written method (email or webform).

Transfers to business units
Recording will ordinarily cease upon transfer from the Customer Service Centre unless the receiving business unit is authorised to continue recording. Where recording may continue, the officer will inform the caller and respect any opt-out request before recording proceeds.

Authorisation for business unit recording
Any business unit intending to record incoming calls—either received directly or transferred from the Customer Service Centre—must obtain prior approval from the relevant Manager and ensure a compliant collection notice and opt-out option is in place.

Compliance with privacy obligations
All principles, processes, and practices involving the recording of calls have been developed in accordance with Council's obligations under the *Privacy and Data Protection Act 2014 (Vic)* and the applicable Information Privacy Principles.

7. Body Worn Cameras, CCTV and Surveillance

7.1 Body Worn Cameras

Council uses body worn cameras (BWCs) worn by Authorised Officers, including Parking Officers and Local Laws Officers, in the course of carrying out their official duties.

BWCs may collect audio and visual recordings that constitute personal information, and in some circumstances sensitive information. Council collects, uses, stores and discloses BWC footage in accordance with the *Privacy and Data Protection Act 2014 (Vic)*, the *Health Records Act 2001 (Vic)* (where applicable), the *Surveillance Devices Act 1999 (Vic)*, and this Policy.

The primary purposes of BWCs are to support officer safety, lawful enforcement activities, evidence collection, and the investigation of incidents or complaints.

The use, operation, access, retention and disposal of body worn camera footage is governed by Council's Body Worn Camera User Guidelines and relevant records management requirements. Access to footage is restricted to authorised personnel and subject to appropriate safeguards.

Requests for access to body worn camera footage, including by individuals captured in recordings, are managed in accordance with the *Freedom of Information Act 1982 (Vic)* and applicable privacy exemptions.

7.2 Public Place CCTV

Council operates a public place CCTV system at various locations across the municipality to support community safety and assist Victoria Police with law enforcement activities.

Signage indicating the presence of CCTV cameras is displayed in all areas where cameras are operating.

Only Victoria Police have access to public place CCTV footage. Any queries about public place CCTV footage need to be directed to Victoria Police.

Council may also use:

- Time-lapse photography at construction sites for project monitoring purposes
- Drone technology for building maintenance monitoring, environmental surveys, and promotional purposes

All data collected by Council from, drones, and time-lapse photography will be used, stored, accessed, disclosed, and disposed of in accordance with the *Privacy and Data Protection Act 2014 (Vic)*, the *Surveillance Devices Act 1999 (Vic)*, and any other relevant legislation.

Further information is available in Council's Public Place CCTV Policy.

7.3 CCTV in Council Buildings

Council operates CCTV systems within certain buildings that it owns, occupies, manages or leases, including staff only workplaces and facilities accessed by both staff and the public (such as municipal offices, libraries, leisure and community facilities, and markets).

CCTV is used for limited and legitimate purposes, including safety and security, protection of Council assets, investigation of unlawful or anti-social behaviour, and incident or complaint management.

Signage is used to indicate where CCTV is in operation so individuals are aware of surveillance before entering monitored areas.

CCTV footage may contain personal information and is handled in accordance with this Policy, the *Privacy and Data Protection Act 2014 (Vic)* and the *Surveillance Devices Act 1999 (Vic)*.

The installation and operation of CCTV in Council buildings is governed by Council's CCTV in Council Buildings Policy and associated procedures, with access restricted to authorised personnel.

Individuals may seek access to CCTV footage containing their personal information in accordance with the *Freedom of Information Act 1982 (Vic)* and applicable privacy exemptions.

8. Use of Artificial Intelligence

Council may use artificial intelligence (AI) tools and systems, including third-party AI services such as Microsoft 365 Copilot, in the delivery of its services and functions.

Council is committed to using AI responsibly and in accordance with applicable privacy legislation. Where AI tools are used, Council will:

- Ensure use aligns with the *Privacy and Data Protection Act 2014 (Vic)* and *Health Records Act 2001 (Vic).*
- Consider privacy implications when procuring or implementing AI tools that may handle personal information
- Rely on contractual and data processing agreements with third-party AI providers to manage privacy obligations

Council staff using AI tools must comply with Council's Use of Artificial Intelligence Policy and other supporting guidelines on the responsible use of AI. In particular, staff must not enter personal or

health information into external AI systems unless the system has been approved for such use and appropriate safeguards are in place.

Clinical or health information, including Maternal and Child Health clinical notes, health information collected through Council-run children's services, and other sensitive case management or safety-related records, must not be entered into AI tools or used for AI-based summarisation, analysis or decision-making.

9. Requests for Access and Correction

Requests for access to and correction of documents containing personal or health information are generally managed under the *Freedom of Information Act 1982 (Vic)*, particularly where requests are complex, contested, or involve exemptions.

However, where appropriate, requests for access to an individual's own personal information may be managed informally outside the FOI Act. Individuals are encouraged to contact Council's Privacy Officer on (03) 9209 6777 or via helpprivacy@portphillip.vic.gov.au to discuss your requirements and the most appropriate pathway.

Requests under the *Freedom of Information Act 1982 (Vic)* must be made in writing, stating as precisely as possible what information is required or needs correction, and be addressed to:

Freedom of Information Officer
City of Port Phillip
Private Bag No. 3
PO St Kilda VIC 3182

Email: helpfoi@portphillip.vic.gov.au

Where a person requests Council to correct their health information, Council will take reasonable steps to notify the person of the decision on the request as soon as practicable, or within 30 days of the request being received.

10. Privacy Complaints and Enquiries

Any person who believes Council has breached their privacy or mishandled their personal or health information may make a complaint to Council's Privacy Officer.

Complaints should be made in writing to ensure Council can properly understand and respond to the issues raised. Council will provide reasonable assistance to any person who requires help to make a written complaint.

Complaints will be acknowledged within two business days and will be resolved as soon as practicable.

Enquiries and complaints may be directed to:

Privacy Officer

City of Port Phillip
Private Bag No. 3
PO St Kilda VIC 3182

Telephone: (03) 9209 6777
Email: helpprivacy@portphillip.vic.gov.au

If a person does not receive a response, or is dissatisfied with Council's response, they may lodge a complaint with the Office of the Victorian Information Commissioner (OVIC).

Office of the Victorian Information Commissioner
Phone: 1300 006 842
Email: enquiries@ovic.vic.gov.au
Post: PO Box 24274, Melbourne VIC 3001

Complaints regarding health information may also be directed to the Health Complaints Commissioner:

Health Complaints Commissioner
Phone: 1300 582 113
Website: hcc.vic.gov.au

Note: The relevant Commissioner may decline to consider a complaint if the matter has not first been raised with Council.

11. Privacy Breaches

A privacy breach occurs when personal, sensitive, or health information is lost, or subject to unauthorised access, use, modification, disclosure, or otherwise handled in an unauthorised or inappropriate manner.

Immediate Response Requirements

Any Council Officer who becomes aware of a suspected or actual privacy breach must:

- immediately take steps to contain the breach, including securing or recovering the information where possible
- ensure the matter is escalated without delay to Council's Privacy Officer
- notify their direct supervisor without delay

The Privacy Officer will provide guidance on containment, risk assessment, and any further investigation.

Councils Privacy Breach Response Process

Council manages privacy breaches through a clear and coordinated process. This process ensures that incidents are contained, assessed, and communicated where appropriate, and that they are reviewed to implement improvements and mitigation measures that reduce the likelihood of future breaches or recurrence. The four steps are:

1. **Contain the breach and conduct an initial assessment**
   Immediately take steps to limit further exposure of personal information and gather preliminary details about what occurred, what information is affected, and who is involved.
2. **Assess the risks associated with the breach**
   Evaluate the potential impact on affected individuals, including the sensitivity of the information, likelihood of misuse, and any vulnerabilities created by the breach.
3. **Determine whether notification is required**
   Consider whether affected individuals, Council leadership, or relevant authorities (such as OVIC) should be notified based on the risk assessment and Council's legal and policy obligations.
4. **Review the incident and implement improvements**
   Identify the root cause of the breach, document lessons learned and implement corrective or preventative actions to reduce the likelihood of similar incidents occurring in the future.

The Privacy Officer will assess each incident and determine whether the breach must be reported to the Office of the Victorian Information Commissioner (OVIC) based on the applicable Business Impact Level (BIL) rating and will provide that report where required.

All privacy breaches are reported to the Executive Leadership Team, included in the Chief Executive Officer's report to Council, and reported to both the Strategic Risk Internal Audit Committee and Audit and Risk Committee for oversight and monitoring.

Breaches of this Policy may result in appropriate disciplinary or remedial action, in accordance with Council's Employee Code of Conduct, Councillor Code of Conduct, or relevant contractual arrangements.

12. Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a structured, step-by-step process that helps Council to identify and assess privacy risks arising from projects, systems or business changes, and determine how those risks can be mitigated or managed.

Council staff must undertake a PIA where a project, initiative or business change is likely to introduce new or changed handling of personal or health information, or where privacy risks are otherwise elevated.

In particular, a PIA is expected to be completed for activities that involve one or more of the following:

- the implementation of new or significantly changed projects, systems or services involving personal or health information
- procurement of new technology, applications or digital services that process or store personal or health information
- establishment or modification of data-sharing arrangements with external organisations or service providers
- significant changes to existing processes or practices that affect how personal or health information is collected, used, disclosed or stored
- implementation of artificial intelligence (AI), machine learning or automated decision-making systems, particularly where these may affect individuals' rights, entitlements or access to services

PIAs are intended to support early identification and mitigation of privacy risks and should be completed at the planning or design stage, before implementation or go-live, wherever practicable.

Where a project does not meet the thresholds outlined above but may still involve residual privacy risk, Council staff are encouraged to undertake a Privacy Impact Assessment (PIA) to support the identification, assessment and management of those risks.

Council's Privacy Officer can provide advice and guidance on when a PIA is required and support staff to complete PIAs in a proportionate and fit-for-purpose manner. A standard PIA template and supporting guidance are available on Council's Intranet or on request to the Privacy Officer.

PIAs form part of Council's broader privacy governance and assurance framework and may be reviewed as part of compliance testing, audit activities or risk management processes to ensure privacy risks are appropriately identified and managed.

13. Staff Training

Information privacy training is mandatory for all employees and other persons engaged by Council.

All new staff members are required to complete privacy training as part of their induction program. Staff must complete the training before handling personal or health information.

All staff are required to undertake refresher training every two years.

Council also offers targeted privacy training to specific work areas on request.

A copy of this Policy is available to all staff via Council's intranet and is also available on Council's website.

Training completion rates are monitored and reported to the Executive Leadership Team monthly.

14. Roles and Responsibilities

Party	Responsibilities
Council Officers (employees), Councillors, Contractors, Agency Staff, Consultants and volunteers	Implementation and awareness of this Policy as individuals and across teams. Creating a strong privacy culture. Completing mandatory privacy training. Reporting potential breaches immediately to supervisor. Following relevant service-specific instructions and approved digital system requirements for collecting, recording, storing, using and sharing personal and health information as part of their role.
Managers	Ensuring staff understand and comply with this Policy. Developing procedures for their service areas that incorporate privacy requirements. Authorising any phone call recording in their area. Notifying Privacy Officer of breaches.
Privacy Officer	Providing advice and guidance on privacy matters. Preparing and periodically updating this Policy for approval. Coordinating privacy training and communications across the organisation. Investigating and responding to complaints. Managing breach responses. Liaising with OVIC and the Health Complaints Commissioner. Supporting compliance assurance activities, including contributing to privacy-related audits and attestations as required.
Freedom of Information Officer	Managing requests for access to and correction of personal information and ensuring decisions balance transparency with privacy protections.
Head of Governance	Overall corporate management of information privacy. Responsible for reviewing and making necessary amendments to this Policy. Ensuring Council meets its legislative obligations.
Digital and Technology Services	Management of ICT security controls and technical safeguards. Management of records and information management systems. Ensuring cloud services comply with privacy requirements.
Senior Governance Compliance Advisor	Conducting annual compliance assessments.

Executive Leadership Team	Providing leadership on privacy culture. Receiving breach reports.

15. Related Council Documents

The following policies, procedures, guidelines, and supporting documents relate to this Policy:

- Asset Management Policy
- Business Continuity Plan
- CCTV in Council Buildings Policy
- Public Places CCTV Policy or CCTV Surveillance Policy
- Child Safety Policy
- Community Engagement Policy
- Councillor Model Code of Conduct
- Cyber Security Incident Register
- Employee Code of Conduct
- Gender Equality Statement of Commitment
- Health and Safety Policy
- ICT Disaster Recovery Plan
- ICT User Policy
- Identity and Access Management Framework
- Information Security Policy
- Information Security Plan
- Information Security Incident response plan
- Non-Compliance Breach Register
- Onboarding and Offboarding processes
- Payment Card Compliance Policy
- Payment Card Data Handling Guidelines
- Protective Security Policy
- Public Transparency Policy
- Records and Information Policy
- Records Disaster Recovery Plan
- Risk Management Framework
- Risk Management Policy
- Social Media and Media Policy
- Use of Artificial Intelligence Policy

16. Related Legislation

- *Privacy and Data Protection Act 2014 (Vic)*
- *Health Records Act 2001 (Vic)*
- *Freedom of Information Act 1982 (Vic)*
- *Public Records Act 1973 (Vic)*
- *Local Government Act 2020 (Vic)*
- *Local Government Act 1989 (Vic)*
- *Planning and Environment Act 1987 (Vic)*

- *Building Act 1993 (Vic)*
- *Surveillance Devices Act 1999 (Vic)*
- *Victorian Charter of Human Rights and Responsibilities Act 2006 (Vic)*
- *Child Wellbeing and Safety Act 2005 (Vic)*
- *Equal Opportunity Act 2010 (Vic)*
- *Workplace Injury Rehabilitation and Compensation Act (Vic)*
- *Occupational Health and Safety Act (Vic)*
- *Family Violence Protection Act 2008 (Vic)*
- *Privacy Act 1988 (Cth)*

16.1 Maternal and Child Health Practice Frameworks

The City of Port Phillip delivers Maternal and Child Health (MCH) services in accordance with Victorian legislation and recognised sector practice frameworks, including the Victorian Maternal and Child Health Program Standards, Department of Health MCH Practice Guidelines, MCH Service Guidelines, and Australian Immunisation Register requirements (where applicable). These frameworks guide Council's approach to service delivery and inform the lawful, secure and sensitive handling of personal and health information associated with MCH services, alongside Council's obligations under this Policy.

16.2 Child Safe

The City of Port Phillip is a Child Safe Organisation and has a legal and moral responsibility to understand and activate their role in preventing, detecting, responding, and reporting any Child Safety concerns. Council has zero tolerance for child abuse and is actively committed to embedding a culture of safety, wellbeing, and inclusion for children and young people.

Consideration has been given to the Child Safe Standards in the development of this Policy, particularly regarding the collection and handling of personal and health information relating to children and young people.

16.4 Gender Equality

Under the *Gender Equality Act 2020*, Council has a positive duty to advance gender equality in our organisation and our community. This includes assessing the impacts of Council's policies on people of different genders, backgrounds, and identities.

In the case of this Policy, a gender impact assessment was not required as the Policy does not directly and significantly impact the community in a manner that would have different effects on different genders.

17. Definitions

Term	Definition
Agent	An individual or organisation engaged by Council to perform a service that involves handling personal or health information.

	An agency relationship means Council will usually be held responsible for how agents handle personal and health information in the same way as its employees.
Clinical Record	Health information recorded by a health practitioner as part of the provision of a health service, including clinical observations, assessments and professional notes. Clinical records are a subset of health information and are governed by the *Health Records Act 2001* and applicable professional standards and service guidelines.
Confidentiality	An obligation owed by the recipient of information to the provider of the information not to disclose or misuse that information. Confidentiality relates to, but is different from, privacy (which is the right of the subject of the information, regardless of who provided or received it).
Consent	Express consent (given explicitly, either verbally or in writing) or implied consent (reasonably inferred from the conduct or circumstances of the individual). Consent must be voluntary, informed, current, and specific to the purpose for which it is given.
Contracted Service Provider	A third party engaged by Council to provide goods or services directly to Council or to the community on Council's behalf. Contracted service providers handling personal or health information are required to comply with the Privacy and *Data Protection Act 2014* and *Health Records Act 2001* through contractual arrangements.
Council	The City of Port Phillip, a municipal Council established under the *Local Government Act 2020 (Vic).*
De-identified Information	Personal or health information that has been altered so that it no longer relates to an identifiable individual or an individual who can be reasonably identified from the information.
Health Information	As defined in the *Health Records Act 2001*, information or an opinion about: (a) the physical, mental or psychological health of an individual; (b) a disability of an individual; (c) an individual's expressed wishes about the future provision of health services to them; (d) a health service provided, or to be provided, to an individual; or (e) other personal information

	collected to provide, or in providing, a health service, or collected in connection with the donation of body parts or substances, or genetic information that is or could be predictive of health.
Health Privacy Principles (HPPs)	The eleven principles established under Schedule 1 of the *Health Records Act 2001 (Vic)* that regulate how Council, as a health service provider, must collect, hold, manage, use, disclose and transfer health information. The HPPs include additional requirements not found in the IPPs, including HPP 10 (Transfer or closure of a health service provider) and HPP 11 (Making information available to another health service provider).
Health Records Act 2001 (Vic)	The Victorian legislation that regulates the handling of health information by health service providers and other organisations in Victoria. The *Health Records Act 2001 (Vic)* establishes the Health Privacy Principles and provides individuals with rights to access and correct their health information.
Health Service	As defined in the *Health Records Act 2001*, an activity performed in relation to an individual that is intended or claimed to: (a) assess, maintain or improve the individual's health; (b) diagnose the individual's illness, injury or disability; (c) treat the individual's illness, injury or disability; or includes a disability service, palliative care service, aged care service, or the dispensing of prescribed drugs by a pharmacist. Council health services include maternal and child health, immunisation, aged care assessment, and community health programs.
Health Service Provider	As defined in the *Health Records Act 2001*, an organisation that provides a health service in Victoria. Council is a health service provider to the extent that it provides health services such as maternal and child health, immunisation, , and disability services.
Immediate Family Member	As defined in the *Health Records Act 2001*, includes a spouse, domestic partner, parent, child, sibling, grandparent, or grandchild of the individual.
Information Privacy Principles (IPPs)	The ten principles established under Schedule 1 of the Privacy and *Data Protection Act 2014* (Vic) that regulate how Council

	must collect, hold, manage, use, disclose and transfer personal information.
Law Enforcement Agency	Includes Victoria Police, the Australian Federal Police, other police services, the Director of Public Prosecutions, and other agencies with law enforcement functions as defined in relevant legislation.
OVIC	The Office of the Victorian Information Commissioner, the independent statutory authority responsible for promoting and overseeing compliance with privacy and freedom of information laws in Victoria.
Personal Information	As defined in the *Privacy and Data Protection Act 2014*, information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Does not include information to which the *Health Records Act 2001* applies.
Primary Purpose	The main purpose, or one of the main purposes, for which personal or health information was collected from an individual. The primary purpose is usually apparent from the context of collection or is communicated to the individual at or before the time of collection.
Privacy and Data Protection Act 2014 (Vic)	The Victorian legislation that regulates the handling of personal information by Victorian public sector organisations, including local councils. The Act establishes the Information Privacy Principles and provides individuals with rights regarding their personal information.
Privacy Breach	An incident involving the unauthorised access to, or unauthorised collection, use, disclosure, or disposal of, personal or health information. A breach may be caused by malicious action, human error, or system failure.
Privacy Collection Notice	A statement provided at or before the time of collection that advises individuals of: (a) the identity of Council and how to contact it; (b) the fact that the individual can access the information; (c) the purposes for which the information is collected; (d) to whom Council usually discloses information of

	that kind; (e) any law requiring the information to be collected; and (f) the main consequences if the information is not provided.
Privacy Impact Assessment (PIA)	A systematic assessment of a project, policy, program, or initiative that identifies the impact it might have on individual privacy and sets out recommendations for managing, minimising, or eliminating that impact.
Privacy Officer	The Council officer designated to provide advice on privacy matters, coordinate privacy training, investigate complaints and breaches, and liaise with OVIC and the Health Complaints Commissioner. At Council, this is the Senior Privacy and Freedom of Information Advisor (Privacy Officer).
Public Interest	A ground that may permit use or disclosure of personal or health information in circumstances not otherwise allowed, where the public benefit outweighs the individual's privacy interest. Public interest disclosures require careful consideration and typically require authorisation by the Chief Executive Officer.
Public Register	A document or database that Council is required by legislation to make publicly available. Public registers may contain personal information and are open to inspection by the public. Examples include registers of building permits and planning permits.
Secondary Purpose	A purpose for using or disclosing personal or health information that is different from the primary purpose for which it was collected. Use or disclosure for a secondary purpose is only permitted in limited circumstances specified in the IPPs and HPPs.
Sensitive Information	As defined in the *Privacy and Data Protection Act 2014*, personal information or an opinion about an individual's: (a) racial or ethnic origin; (b) political opinions; (c) membership of a political association; (d) religious beliefs or affiliations; (e) philosophical beliefs; (f) membership of a professional or trade association; (g) membership of a trade union; (h) sexual preferences or practices; or (i) criminal record.

Serious Threat	A threat to an individual's life, health, safety or welfare, or to public health, public safety, or public welfare, that is both serious in nature and imminent or ongoing. This threshold must be met before personal or health information can be used or disclosed without consent under IPP 2.1(d) or HPP 2.2(h).
Transborder Data Flow	The transfer of personal or health information to a recipient located outside Victoria. Such transfers are only permitted in limited circumstances specified in IPP 9 and HPP 9.
Unique Identifier	A number, letter, or symbol, or a combination of any or all of these, that is assigned by an organisation to an individual to identify uniquely that individual for the purposes of the organisation's operations. Does not include an identifier that consists only of the individual's name.

Attachment 1 - Information Privacy Principles

The following table summarises the ten Information Privacy Principles (IPPs) under the *Privacy and Data Protection Act 2014 (Vic)*:

IPP	Subject	Key Principles
1	Collection	Only collect personal information necessary for functions. Collect by lawful and fair means, not intrusively. Notify individuals of collection purpose, right to access, usual disclosures, any laws requiring collection, and consequences of not providing information.
2	Use and Disclosure	Use or disclose only for primary purpose or related secondary purpose reasonably expected. Otherwise only with consent, for law enforcement, to prevent serious threats, for research (with safeguards), or as required by law. Record law enforcement disclosures.
3	Data Quality	Take reasonable steps to ensure information collected, used, or disclosed is accurate, complete, and up to date.
4	Data Security	Protect from misuse, loss, unauthorised access, modification, or disclosure. Destroy or permanently de-identify when no longer needed.
5	Openness	Document policies on management of personal information and make available on request. Advise individuals generally what information is held, purposes, and how it is handled.
6	Access and Correction	Provide access on request unless exceptions apply (threat to life/health, privacy impact on others, frivolous request, legal proceedings, prejudice to investigation or law enforcement, etc.). Correct inaccurate information. Provide reasons for denial. Respond within 45 days.
7	Unique Identifiers	Only assign where necessary for functions. Do not adopt identifiers from other organisations unless necessary, consented, or required by law. Do not require provision of external identifiers unless authorised.
8	Anonymity	Where lawful and practicable, allow individuals the option of not identifying themselves in transactions.

9	Transborder Flows	Only transfer outside Victoria where recipient has similar protections, individual consents, transfer is necessary for contract, transfer is for benefit of individual, or reasonable steps ensure consistent handling.
10	Sensitive Information	Only collect sensitive information with consent, where required by law, to prevent serious threat to life/health, or for legal claims.

Source: *Privacy and Data Protection Act 2014* (Vic), Schedule 1

Attachment 2 - Health Privacy Principles

The following table summarises the eleven Health Privacy Principles (HPPs) under the *Health Records Act 2001 (Vic):*

HPP	Subject	Key Principles
1	Collection	Only collect health information necessary for functions with consent, as permitted by law, to provide a health service where individual cannot consent, to prevent serious threat, for research (with HCC guidelines), or for law enforcement. Collect by lawful and fair means. Notify of collection matters.
2	Use and Disclosure	Use for primary purpose. Secondary use only if directly related and expected, with consent, required by law, for provision of health services, for health service management/training (de-identified), for research (with safeguards), to prevent serious threat, for investigation of unlawful activity, or for law enforcement. May disclose to immediate family for care/compassion if individual incapable.
3	Data Quality	Ensure health information is accurate, complete, up to date, and relevant to functions.
4	Data Security and Retention	Protect from misuse, loss, unauthorised access. Health service providers must not delete health information unless permitted by law or after retention period (age 25 or seven (7) years after last service). Record deletions and transfers.
5	Openness	Document policies on health information management and access procedures. Make available on request. Advise individuals whether information is held and how to access it.
6	Access and Correction	Provide access via a Freedom of Information request unless exceptions apply. Correct inaccurate information but do not delete - place incorrect information on restricted record. Notify individual of correction decision within 30 days. Provide written reasons for refusal.
7	Identifiers	Are only assigned where reasonably necessary. Private sector organisations generally cannot adopt public sector identifiers unless consented, required by law, or fulfilling obligations to the public sector organisation.

8	Anonymity	Allow individiuals the option of not identifying themselves, when dealing with Council where it is lawful and practicable to do so.
9	Transborder Flows	Only transfer outside Victoria where recipient has similar protections, individual consents, transfer is necessary for contract, for benefit of individual, reasonable steps taken, or authorised by law.
10	Transfer/Closure	If health service is transferred or closed: publish newspaper notice, advise how health information will be dealt with, take steps to notify individuals. After 21 days, elect to retain or transfer information. Retain securely until destruction permitted.
11	Transfer to Provider	On request by individual or authorised provider, make health information available to another health service provider as soon as practicable. May charge prescribed fee.

Source: *Health Records Act 2001 (Vic),* Schedule 1

Attachment 3 - Personal and Health Information Collected by Council

Council may collect the following types of personal information:

- Title, first name, surname
- Address (residential, postal, email)
- Contact telephone numbers
- Date of birth / age
- Gender
- Marital status / domestic partner status
- Signature
- Photographs and video recordings
- Motor vehicle registration numbers
- Audio recordings of telephone conversations (where consent is provided)
- Financial information (for rates, payments, debt collection)
- Employment information (for staff records)
- Customer, account, reference or record numbers allocated or used by Council to administer services
- Health information where Council provides health or wellbeing services (such as medical conditions, immunisation records and immunisation status, disability information, and health management plans)
- Information provided through online forms, digital services, or Council information systems

Council collects personal and health information for functions and services including, but not limited to:

- Rates and property management
- Planning and building permits
- Animal registration and management
- Parking permits and infringement notices
- Library membership
- Venue and sports ground hire
- Community engagement and consultation
- Maternal and Child Health services
- Early years, childcare and kindergarten services
- Immunisation programs
- Aged care and disability services
- Youth services
- Environmental health and food safety
- Local laws enforcement
- Customer enquiries and complaints

- Council meetings and public submissions
- Events and programs
- Staff employment and recruitment
- Insurance claims
- Debt collection

Council upholds Payment Card Industry Security Standards (PCI DSS) and does not store payment card details such as credit card or debit card numbers, except for direct debit arrangements where collection statements confirm use, purpose, and disclosure restrictions.