

Privacy Policy

Responsible officer:	Director Corporate and Organisational Development
Key Result Area:	Governance and Decision Making
Document type:	Policy
Reference:	10/01/0004
Approved by:	Council
Date approved:	23 August 2023
Date of next review:	August 2027

Purpose

Council believes that the responsible handling and protection of personal and health information is a key aspect of democratic governance and is strongly committed to protecting an individual's right to privacy.

The purpose of this policy is to outline how Council delivers on this commitment while ensuring compliance to relevant legislation including the Information Privacy Principles (IPP) as contained in the *Privacy and Data Protection Act 2014* and the Health Privacy Principles (HPP) contained in the *Health Records Act 2001*.

Scope

This Policy applies to any personal or health information held by Council.

Definitions

Term	Meaning
Health Privacy Principles (HPP)	The set of principles from the <i>Health Records Act 2001</i> that regulate the minimum standards when handling personal information for health purposes.
Information Privacy Principles (IPP)	The set of principles from the <i>Privacy and Data Protection Act 2014</i> that regulate the minimum standards when handling personal information.
Personal Information	<p>Personal information means information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.</p> <p>For example, Council holds personal information regarding its ratepayers such as names and addresses in order to carry out its functions (for example planning, valuations, property services, child-care services). In some instances, personal information may be contained on a public register (for example a register of planning permits, food premises or animal registration details).</p>
Sensitive Information	Sensitive information is defined as personal information or an opinion about an individual's race or ethnic origin, political opinions or associations, religious or philosophical beliefs or affiliations, trade union memberships, sexual preferences or practices, criminal record, or their health or genetic information.
External Contractors	Council may outsource some of its functions to third parties (for example immunisations). This may require the contractor to collect, use or disclose certain personal information. It is the intention of Council to require contractors to comply with the IPPs and the provision of the <i>Privacy and Data Protection Act 2014</i> in all respects.
Health Information	Health information includes information about the physical, mental or psychological health, or disability of an individual. It also includes information collected to provide a health service to an individual (such as a disability or aged care service, immunisation service or maternal health care service), including an individual's expressed wishes about the future provision of health services.

Privacy Principles

Principle 1 - Collection

Council will only collect personal and health information that is necessary for specific and legitimate functions and activities of the council. All information will be collected by fair and lawful means and not in an unreasonably intrusive way. This type of information typically includes but is not limited to the following:

- Name
- Address (residential, postal and email)
- Telephone number (work, home and mobile)
- Date of birth
- Occupation
- Medicare number
- Credit card and bank account numbers
- Motor vehicle registration number

Occasionally, information may be provided to Council about an individual from a source other than the individual. If Council collects personal and health information about an individual from someone else, Council will take all reasonable steps to ensure that individual is informed of his or her rights relating to the information collected. This may include for example:

- A third party may provide Council with address change notification, which is used to update customer records; or
- Council may obtain demographic or customer interests information used for planning purposes and understanding customer consumption patterns and behaviour.

When information about an individual is obtained, Council will provide the individual details of:

- Why it is collecting personal and health information;
- How that information can be accessed;
- The purpose for which the information is collected;
- With whom the council shares this information;
- Any relevant laws; and
- The consequences for the individual if all or part of the information is not collected.

Principle 2 - Use and Disclosure

Council will not use or disclose personal and health information for a purpose other than the following:

- For the primary purpose for which it was collected;
- For secondary purposes where these are related to the primary purpose of collection and are reasonably expected;
- In accordance with their consent;
- Where required or authorised under law; and
- Where otherwise permitted by the IPPs and HPPs.

Council may also disclose personal information to:

- Government agencies in accordance with their relevant legislation and functions;
- Statutory authorities to enable them to advise individuals of works which may impact upon them or their property (such as road closures, property acquisition etc.);
- Law enforcement and emergency agencies for emergency or law enforcement purposes;
- Water, gas and electricity utilities for the purposes of ensuring data is accurate;
- Professional advisers, including accountants, auditors, insurers, bankers, valuers,
- Debt collection agencies;
- IT providers and lawyers; and
- Other individuals or organisations where Council believes that the 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, safety or welfare.

Principle 3 - Data Quality

Council will take reasonable steps to make sure that the personal and health information it collects uses or discloses is accurate, complete and up to date.

Principle 4 – Data Security

Council will take reasonable steps to protect all personal and health information it holds from misuse, loss, unauthorised access, modification or disclosure. Council will take reasonable steps to lawfully and responsibly destroy or permanently de-identify personal and health information when it is no longer needed for any purpose as specified in the Acts.

Principle 5 - Openness

Council will make publicly available its policies relating to the management of personal and health information. Council will, on request, take reasonable steps to provide individuals with general information on the types of personal and health information it holds and for what purposes and how it collects, holds, uses and discloses that information.

Principle 6 - Access and Correction

Council will provide access to information held by council about an individual on request except in specific circumstances as outlined within the Act.

Where Council holds personal and health information about an individual and the individual is able to establish that information is incorrect, Council will take reasonable steps to correct information as soon as practicable but within 45 days of the request. If, however, Council denies access or correction, Council will provide reasons.

In the event that Council and an individual disagree about the veracity of personal and health information held by Council, Council will take reasonable steps to record a statement relating to the disputed information if requested by the individual.

Principle 7 - Unique Identifiers

Council will not assign, adopt, use, disclose or require unique identifiers from individuals except for the course of conducting normal council business or if required by law. Council will only use or

disclose unique identifiers assigned to individuals by other organisations if the individual consents to the use and disclosure or the conditions for use and disclosure set out in the Acts are satisfied.

Principle 8 - Anonymity

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

Principle 9 - Transborder Data Flows

Council may transfer personal and health information outside of Victoria only if that data transfer conforms to one of the reasons and conditions outlined in the Acts.

Principle 10 – Sensitive Information

Council will not collect sensitive information about an individual except for circumstances specified under the Acts.

Principle 11 - Transfer or Closure of the Practice of a Health Service Provider

If the health services of Council are to be transferred or closed, Council will take reasonable steps to notify recipients of alternative health services and of the options to transfer their information to the new health service provider or a health service provider nominated by them or retain their own health records.

Principle 12 - Making Information available to another Health Service Provider

Council will upon consent by an individual, provide a copy of or written summary of their health information to a specified health service provider, on payment of a fee not exceeding the prescribed maximum fee and subject to the regulations.

Data and Privacy Breach Procedure

All data and privacy breaches (breaches) must be reported to the Council's Privacy Officer as soon as practicable once a breach is detected via info@towong.vic.gov.au.

Once a breach is reported to the Privacy Officer, the Privacy Officer will work with the relevant Director and/or CEO to conduct a risk assessment of the breach and determine the probability of harm to any person(s) who personal information may have been compromised.

In all cases of breaches, the following response will be implemented:

- **Contain** the breach immediately to prevent any further compromise of personal information;
- **Assess** the risks of harm to affected individuals by investigating the circumstances of the breach;
- **Notify** affected individuals if deemed appropriate in the circumstances; and
- **Review** the breach and the organisation's response to consider longer-term action to prevent future incidents of a similar nature and improve the organisation's handling of future breaches.

If there is a high probability of harm to any person(s) affected, the Privacy Officer will promptly notify the Victorian Information Commissioner of the incident. The affected individuals will also be notified as soon as reasonably practicable and remain transparent throughout the process.

The breach incident will be reported to the Council WHS Officer to be recorded and maintained in the Incident Register, which will be used to record all known breaches.

Deployment

Management and staff will be responsible for the delivery of this policy within their areas of responsibility.

Relevant Legislation

Privacy and Data Protection Act 2014

Health Records Act 2001

Complaints

If an individual feels aggrieved by Council's handling of their personal, sensitive or health information, they may make a complaint to Council's Privacy Officer by email info@towong.vic.gov.au or by post to 'Privacy Officer – Towong Shire Council', PO Box 55, Tallangatta VIC 3700.

The complaint will be investigated as soon as possible (but no later than 5 business days) and a written response will be provided to the individual. Alternatively, the individual may make a complaint to the Victorian Information Commissioner in relation to personal information or the Health Complaints Commissioner in relation to health information. Please note that the Commissioners may decline to hear the complaint if the individual has not first made a complaint to Council.

Further Information

The Office of the Health Complaints Commissioner can be contacted by telephone on 1300 582 113.

The Office of the Victorian Information Commissioner (OVIC) can be contacted by telephone on 1300 006 842.

Human Rights Charter Compatibility

This policy has been assessed as being compatible with the *Charter of Human Rights and Responsibilities Act 2006 [Vic]*.

Results

The deployment of this policy and the results achieved will be reviewed annually.



Authorised by:

Juliana Phelps

Chief Executive Officer