



1.0 AUTHORITY

- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*

2.0 INTENT

The purpose of this policy is to set out the Mornington Peninsula Shire's (the Shire) framework for management of the personal and health information it holds, and to meet the requirement under Information Privacy Principle (IPP) 5 of the *Privacy and Data Protection Act 2014*, and Health Privacy Principle (HPP) 5 (openness) of the *Health Records Act 2001* to have a clearly expressed and accessible policy showing how the Shire manages personal and health information.

3.0 SCOPE

This policy applies to Councillors, Shire employees, volunteers and contractors and includes all personal and health information held by the Shire.

4.0 GOVERNANCE PRINCIPLES

Under the *Local Government Act 2020*, Council must give effect to the following overarching governance principles:

- a) Council decisions are to be made and actions taken in accordance with the relevant law;
- b) priority is to be given to achieving the best outcomes for the municipal community, including future generations;
- c) the transparency of Council decisions, actions and information is to be ensured.

5.0 POLICY STATEMENT

The Shire is committed to ensuring the personal and health information it holds is managed in accordance with the *Privacy and Data Protection Act 2014*, the *Health Records Act 2001* and the IPP and HPP principles contained in those Acts (the Acts).

5.1 Collection of Personal and Health Information

The Shire will only collect personal and health information that is necessary for carrying out its functions and activities. Where reasonable and practicable, it will collect the information directly from the individual and will do so by fair and lawful means and not in an intrusive way.

The Shire will only collect sensitive information where the individual has consented or as permitted under legislation.

If the Shire collects personal or health information about an individual from someone else, it will take reasonable steps to ensure that the individual is aware their information has been collected.



Audio and Visual Recordings

The Shire may take photographs, video or audio recordings both on Shire premises and in public places. These recordings may be used for Shire activities such as local law enforcement, publicity or recording and broadcasting of Council meetings and Shire events.

For recordings taken for publicity purposes, consent will be sought (if practicable) from individuals prior to taking the recordings. Where practicable, consent will be obtained in writing using a consent form. During public events or in public places, it may not be practicable to obtain individual consent forms. In such cases, the Shire may use other methods to inform individuals that recordings are being taken and how they will be used. This may include public signage, announcements and flyers. Such methods will inform individuals that they may be recorded and provide them the opportunity to inform Shire staff/photographers that they don't want their image or recordings of them used for such a purpose.

Closed Circuit Television Cameras (CCTV)

CCTV cameras are used at Shire buildings, including municipal offices, recreation centres and youth centres to increase security, reduce crime and promote community safety. Recordings made by these cameras are subject to the IPPs and HPPs and will only be viewed by authorised people and for the purposes stated above.

Body Worn Cameras

Body worn cameras are used by Shire Authorised Officers (AO) to assist in the deterrence, prevention and monitoring of incidents involving AO's interactions with members of the public, to improve safety in the workplace and to assist with investigations conducted by AO. AO may make recordings of members of the public using a body worn camera when:

- exercising an authorised legislated power and where the recording would assist in collecting evidence; and
- any other occasion when the AO believes a recording is necessary:
 - that an offence is being committed, has been committed or is about to be committed, or
 - that would provide transparency of a public interaction, or
 - enforcement or non-compliance activity.

When making recordings, AO will inform members of the public at the earliest opportunity that they are being recorded unless it is not practicable or there is an occupational health and safety issue occurring.

The use of body worn cameras is in accordance with the *Surveillance Devices Act 1999* and any recordings made using body worn cameras are managed in accordance with the *Privacy and Data Protection Act 2014*.

Shire Websites, Online Forums and Social Media

The Shire uses social networking services (e.g. Facebook, Twitter), online forums (e.g. Your Say) and other websites to connect with the community and residents. This includes responding to customer enquiries, promoting Shire assets and services, and community consultation and feedback.



Any public social media and website commentary on Shire social media accounts, online forums and websites is accessible by the public. Any public commentary may also be used by the Shire in its publications in relation to community consultation, feedback and enquiries.

To protect individual's privacy and the privacy of others, personal or health information including phone numbers or email addresses are not to be included. Individuals are asked not to share personal or health information about others. Any personal or health information collected by the Shire will be handled in accordance with this policy and the Digital Communications Policy.

Third-party social media services and websites (e.g. Facebook, Twitter) also handle personal information for its own purposes. It is recommended individuals review their privacy policies to understand how personal information is managed.

Collection Notices

Whenever the Shire collects personal or health information, a collection notice will be provided outlining how it will use and handle the information. Collection notices may be provided in a number of ways, including verbally such as during phone calls, in writing on forms or the Shire's website, signage displayed at events where recording is taking place.

5.2 Use and Disclosure of Personal Information

The Shire will only use personal and health information for the purpose it was collected for, or for a related secondary purpose that could reasonably be expected.

The Shire will not disclose personal or health information unless:

- the Shire has obtained the consent of the individual;
- the Shire is required or authorised by law to do so;
- the information is necessary for the Shire or a law enforcement agency to perform its functions, duties and activities (including, but not limited to, the prevention, detection, investigation, prosecution or punishment of criminal offences);
- the disclosure is necessary for research, or the compilation or analysis of statistics in the public interest (in which case personal information will be de-identified); or
- the Shire believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety of a person, or to public health, safety or welfare

The information may be disclosed to:

- the Shire's contracted service providers who manage services provided by the Shire. Some examples include garbage collection, management of leisure centres, environmental health inspections and infrastructure maintenance. The Shire will also require these service providers to maintain the confidentiality of the information and comply with the IPPs and HPPs.
- Shire appointed committees for the purpose of achieving their objectives.
- an individual's authorised representatives, health service providers or legal advisers.
- the Shire's professional advisers, including accountants, auditors and lawyers.



- organisations assisting the Shire to perform statistical analyses for improving the services being delivered to the community. However, where practicable and reasonable, steps will be taken to de-identify the information.
- government agencies and other organisations, with the specific consent of the individual, or where required or authorised by law, which may include emergency situations and assisting law enforcement agencies.
- an immediate family member of the individual, for compassionate reasons or if it is necessary to provide the appropriate care or health service to the individual, when permitted by law
- any recipient outside Victoria, only if they are governed by substantially similar information privacy principles, or when the individual has consented to the transfer or would be likely to give it, if it was practicable to obtain that consent.

Personal and health information will be disclosed by the Shire where required to do so by any other legislation. Where there is an inconsistency, all other legislation overrides the Acts to the extent of the inconsistency. Other obligations under the Acts will remain.

5.3 Data Quality, Security and Retention

The Shire will take all reasonable steps to ensure the personal and health information it collects, uses or discloses is accurate, complete and up-to date.

The Shire will maintain secure systems for storing personal and health information. Technological and operational policies and procedures will be implemented to protect information from misuse and loss and from unauthorised modification or disclosure.

The Shire will dispose of personal and health information where it is no longer necessary to fulfil the purposes for which the information was collected or as required by law.

The Shire will process and handle payment card data in accordance with the Payment Card Industry Data Security Standards and will not store payment card details once processed and not transmit payment card details via email.

5.4 Accessing, Updating and Deleting Personal and Health Information

Individuals can request to access or update their personal or health information by contacting the Shire's Freedom of Information Officer via email foi@mornpen.vic.gov.au or phone 5950 1355.

Individuals can request their personal and health information held by the Shire be deleted by contacting the Shire's Privacy Officer via email privacy@mornpen.vic.gov.au. Requests for deletion of personal and health information will be met by the Shire unless it is legally permitted to refuse to do so, in which case details of the refusal will be provided to the individual in writing.



5.5 Unique Identifiers

A unique identifier is a number or code assigned for the primary purpose of identifying an individual, for example a driver's licence number or a tax file number. The Shire will only assign unique identifiers to individuals if it is necessary to enable its functions to be carried out efficiently.

5.6 Anonymity

Where lawful and practicable, individuals will have the option of transacting with the Shire without identifying themselves. For example, customers can make an anonymous complaint. However, if an individual chooses not to provide certain information, the Shire may not be able to adequately respond to their correspondence or request.

5.7 Trans-border Data Flow

The Shire may transfer personal and health information to an individual or organisation outside Victoria only in limited circumstances:

- If the individual has consented; or,
- If disclosure is authorised by law; or,
- If the recipient of the information is subject to a law, binding scheme, or contract with privacy principles that are substantially similar to those in the Acts.

Where the Shire utilises cloud computing services outside Victoria or engages a contractor who stores their data outside Victoria, all reasonable steps will be taken to ensure that the service provider or contractor will manage the personal and health information in accordance with the Victorian IPPs and HPPs. This includes ensuring that the recipient of the information is subject to laws and/or binding contractual arrangements that provide similar protections afforded by the Acts.

5.8 Sensitive Information

The Shire will only collect sensitive information about an individual where the individual has consented or when it is required or authorised by law.

5.9 Privacy Breaches

Upon becoming aware of a breach or potential breach of the IPPs or HPPs, employees will notify their direct supervisor immediately. Upon confirming that a breach has occurred, the direct supervisor shall notify both the relevant manager and the Shire's Privacy Officer.

In responding to a breach, the Privacy Officer will be guided by advice provided by OVIC in the guidelines Managing the Privacy Impacts of a Data Breach and the Shire's Guidelines for Responding to Privacy Breaches.



The Shire will, in accordance with its obligations under the Commonwealth *Privacy Act 1998* as a Tax File Number Recipient, notify the Australian Information Commissioner and affected individuals of eligible data breaches involving tax file numbers.

5.10 Privacy Complaints

If there are concerns about the way the Shire has handled personal or health information or an individual believes their privacy has been breached, a complaint can be made to the Shire's Privacy Officer. Further information about making a privacy complaint can be found on the Shire's website [Privacy Statement - Mornington Peninsula Shire \(mornpen.vic.gov.au\)](https://mornpen.vic.gov.au/Privacy-Statement).

Alternatively, a complaint may be made to the Office of the Victorian Information Commissioner (OVIC) for personal information, or to the Health Complaints Commissioner (HCC) for health information. This includes where an individual is not satisfied with the way the Shire has handled their complaint. OVIC's website www.ovic.com.au and HCC's website www.hcc.vic.gov.au provides information on making a complaint to their offices.

It should be noted that the respective Commissioner may decline to hear a complaint if it has not first been raised with the Shire.

6.0 HUMAN RIGHTS CHARTER COMPATIBILITY

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

7.0 ASSOCIATED DOCUMENTS

- Employee Code of Conduct
- Councillor Code of Conduct
- Security of Council and Councillor Documentation Policy
- Record Keeping Policy
- Closed Circuit Television Policy
- Digital Communications Policy
- Employment Checks Policy
- Guidelines for Responding to Privacy Breaches.
- Payment Card Industry Data Security Guidelines
- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- *Freedom of Information Act 1982*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Surveillance Devices Act 1999*

8.0 DEFINITIONS

Personal Information

Information or an opinion (including information or an opinion forming part of a database), recorded in any form and whether true or not,



about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Health Information

Health information is any information or opinion about a person's health or disability, and any information that relates to a health service they have received or will receive.

Sensitive Information

Information or an opinion about an individual's

- racial or ethnic origin,
- political opinions,
- membership of a political association, religious belief or affiliations, philosophical beliefs,
- membership of a professional or trade association,
- membership of a trade union,
- sexual orientation or practices,
- criminal record.

Authorised Officer

and that is also personal information.

A person, other than a Councillor, appointed by council to carry out a compliance function or an enforcement function under legislation related to the functions and powers of the Council

Body Worn Camera

A portable camera, mounted on the body and used by AOs to capture audio and video recordings of interactions between officers and the public.

9.0 POLICY SPONSOR

The Manager – Legal and Governance is responsible for overseeing the application and review of the Privacy policy.

10.0 DOCUMENT CONTROLS

This policy will be reviewed within three years from the date of adoption, no later than (insert date)

Administrative Updates

It is recognised that, from time to time, circumstances may change leading to the need for minor administrative changes to this document. Where an update does not materially alter this document, such a change may be made administratively. Examples include a change to the name of a Council department, the change to an existing policy or document referred to in this policy, and minor updates to legislation and the like which does not have a material impact. However, any change or update which materially alters the document must be by approval of the Executive Team.