POLICY

C028 Privacy and Data Protection Policy

1 Purpose

The purpose of this policy is to support Hindmarsh Shire Council in meeting its obligations under the *Privacy and Data Protection Act 2014* in the collection, management, and disclosure of personal information, and to ensure that the Information Privacy Principles are embedded in our operational environment.

2 Scope

This policy applies to all Councillors, employees, contractors, and volunteers of Council.

This policy applies to all personal information held by Council, including information sourced by Council from third parties.

Third Party Contractors Bound by Act

Where a contractor of Council breaches the Information Privacy Principles (IPPs), Council will be held responsible unless the contractor has agreed to be bound by the IPPs in an enforceable contract with the Council.

For this reason, all new contracts should include a provision ensuring that third party contractor, including subcontractors to them, are bound by the IPP's in the same way and to the same extent as Council. Model Terms to be used in contracts, MOU's and/or agreements have been included in section 4.13 of this policy.

To assist with compliance the contractor must be provided with a copy of this policy.

3 Definitions

Council	means Hindmarsh Shire Council
IPPs	means Information Privacy Principles
PDPA	means the *Privacy and Data Protection Act 2014*
Personal information	means information or an opinion about an individual whose identity is obvious or can reasonably be established, other than certain health or generally available information.
Policy	means this Privacy and Data Protection Policy

Primary Purpose	means the purpose/s for which an individual's personal information was collected.
Secondary Purpose	means a purpose related to the primary purpose; or where an individual would reasonably expect Council to use or disclose their personal information.

4 Policy Statement

Council seeks to responsibly manage the personal information it handles and is committed to ensuring full compliance with the IPPs outlined in the PDPA. Council believes that the responsible handling of personal information is a key aspect of democratic governance and is strongly committed to protecting an individual's right to privacy.

4.1 Principle 1 - Collection

4.1.1 The Type of Information Collected

The type of personal information collected by Council will depend on the functions, services, events, and activities offered by Council. The personal information Council typically collects includes, but is not limited to an individual's:

- name
- date of birth
- address
- contact information (email & phone number)
- signature
- vehicle registration number
- payment or billing information

Council will only collect personal information that is necessary for carrying out its functions or activities. Before collection occurs, Council staff must have established the type of personal information they will be collecting and confirm that all personal information proposed to be collected is required for the program, service, or activity they provide. Collecting personal information with no identifiable purpose is not acceptable.

Council must collect personal information only by lawful and fair means and not in an unreasonably intrusive way. Council must have the appropriate power to collect the information it is requesting and that there are no other laws prohibiting such collection.

Information has been collected unfairly if it was obtained by trickery, misrepresentation, deception or under duress. For example, information would have been collected by unfair means if Council knowingly accepts personal information from someone who it knows is under the mistaken belief that they have no choice but to provide said information.

4.1.2 Informed Consent for Collection

Council must take reasonable steps to provide the individual with full information regarding the collection by including a collection notice at the point of collection stating:

- why Council is collecting personal 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.

The following collection notice applies to all personal information collected by Council unless specifically stated otherwise:

Hindmarsh Shire Council collects personal information to enable us to perform our statutory functions and provide services, activities and events. Council stores personal information in secure information technology systems and shares information, only when necessary, amongst internal work areas (including contractors) to facilitate a more efficient customer experience across Council's business. If the personal information is not collected, Council may not be able to provide you with Council services, discharge our functions or keep you updated on the progress of your service request.

We will handle any personal information you have provided in this form in accordance with the Privacy and Data Protection Act 2014*. Our privacy policy contains information about how you may access your personal information and seek correction of such information; as well as how to complain about a breach of the Australian Privacy Principles and how we will deal with such a complaint. For more information, please see our Privacy Policy or contact our team on (03) 5391 4444. Your personal information will not be disclosed to any other party unless Council is required to do so by law, has gained your consent to do so or an information privacy principle exemption applies.*

4.1.3 Direct Collection and Anonymity

Under normal circumstances Council must collect personal information about an individual only from that individual. This enables individuals to have some control over what is collected, by whom and for what purpose. Direct collection provides the individual with the opportunity to refuse to provide their information. It also makes it more likely that the information collected by Council is relevant, accurate and complete. Information may be collected from a third party where that party has legal authority to act on the primary person's behalf.

However, if Council collects personal information about an individual from someone else, Council must take all reasonable steps to ensure that individual is informed of their rights relating to the information collected.

Where lawful and practicable, Council will offer a person the option of remaining anonymous as part of a transaction with Council. However, as anonymity may limit Council's ability to process a complaint or other matter, Council reserves the right to take no action on any matter where a person chooses not to supply relevant personal information so that it can perform its functions.

4.1.4 Website Third Party Providers

Council uses various external applications to conduct online surveys, send newsletters, reserve tickets, book Council services and measure website use. These external providers may also collect your personal information. To ensure that you are fully informed on how any personal information is being collected it is recommended you read the privacy policy of the third-party provider prior to participating. Following is a list of current third-party providers used on Council's website and/or by Council's Committees:

- Mailchimp

- Jotform
- Engagement HQ
- TryBooking
- Eventbrite
- eProcure

4.1.5 Social Media

Council uses Facebook, Instagram, and YouTube to communicate with the public. To protect your own privacy and the privacy of others please do not include any personal information including phone numbers and email addresses. The social networking services will also handle your personal information for its own purposes. These sites have their own privacy policies that users should be aware of.

4.1.6 Visual Surveillance Devices

Corporate Surveillance Devices and Systems installed in public spaces, on council facilities and land.

These systems are managed and monitored by Council employees or contractors. This includes but is not limited to Council offices, pools, libraries, community halls, public toilets, sporting grounds, and waste management facilities.

These devices are used to:

- Support and implement broader crime prevention and reduction strategies;
- Enhance actual and perceived safety and security for staff and users of Council facilities;
- Discourage damage and vandalism of Council assets;
- Detect and manage any illegal activities on Council facilities and land (eg rubbish dumping or graffiti);
- Enhance site security and security for equipment at Council construction sites;
- Support legislated responsibilities and operational business (eg aerial mapping for fire prevention);
- Assist with traffic planning and road management such as traffic counts on local roads;
- Enhance biodiversity activities, such as wildlife monitoring and pest animal control in local bushland and parks;
- Monitor any unauthorised access to ‘staff only’ areas; and
- Record and promote Council events.

4.2 Principle 2 – Use and Disclosure of Information

Council will take all necessary measures to prevent unauthorised access to, or disclosure of, personal information. Council will only use personal information within Council or disclose it outside of Council for the purpose for which it was collected, unless one the following apply:

- where Council has a person’s consent
- for a related secondary purpose a person would reasonably expect
- or as required or permitted by the PDPA or any other legislation.

Council will only use personal information within Council, or disclose it outside Council:

a) for the primary purpose it was collected;
b) in accordance with legislative requirements;

c) for a secondary purpose with the consent of the individual concerned; or
d) for a secondary purpose related to the primary purpose where an individual would consider it reasonable to do so

The majority of personal information collected by Council is collected to enable Council to perform our statutory functions and provide services, activities and events. As the responsibilities for many of Council's functions and services often overlap between department's internal disclosure, and external disclosure to contracted service providers, of personal information is necessary to satisfactorily perform this primary purpose.

Secondary purposes for use and disclosure must be related (or, in the case of sensitive information, directly related) to the primary purpose of collection AND consistent with what an individual would reasonably expect. Reasonableness requires that the related secondary use or disclosure is also proper and fair, and generally not incompatible with the primary purpose of collection. When establishing 'reasonably expected' you must ask what an ordinary person, not an expert in local government would consider reasonable.

4.2.1 Other Departments within Council

Personal information will be disclosed internally to other work areas within Council to assist in the efficient actioning of enquiries. The personal information (contact details) contained in the single customer view may also be used to liaise with the customer in relation to the delivery of other Council services.

4.2.2 Contracted Service Providers

Council outsources some of its functions and services to third party contractors who perform them on Council's behalf. To enable this to occur efficiently, Council may disclose personal information we have collected about an individual to the contractor. Council will only disclose the personal information if it is necessary for the contractor to carry out its specific task.

All contracts with contracted service providers should require contractors be bound by the IPP's in the same way and to the same extent as Council. All contracted service providers should also be provided with a copy of this policy.

4.2.3 Legislation and Law Enforcement

The disclosure of personal information by Council in accordance with legislative requirements is not a breach of the Information Privacy Principles.

Personal information may also be contained in Council's Public Registers. Under the *Local Government Act 1989*, any person is entitled to inspect Council's public registers, or make a copy of them, upon payment of the relevant fee. Council maintains the following public registers containing personal information:

- Details of overseas or interstate travel undertaken in an official capacity by Councillors or any Council employee in the previous 12 months
- Register of interests kept under section 81 of the Act
- Record of persons who inspect the register of interests (limited inspection rights)
- Minutes of meetings of special committees established under section 86 of the Act and held in the previous twelve months
- Register of delegations kept under sections 87, 88 and 98 of the Act
- Register of leases entered into by Council
- Register of authorised officers appointed under section 224 of the Act

- A listing of donations and grants made by Council during the financial year including the names of recipients and the amounts received
- Register of election campaign donation returns
- Register of Planning Permits
- Register of Building Permits
- Register of all registered dogs and cats
- Written record of an assembly of Councillors

Council may also disclose personal information to law enforcement agencies, including the courts and Victoria Police, if it believes that the disclosure is reasonably necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction.

4.2.4 Submissions to Council

Council believes in an ongoing dialogue between the community and Council. As such, Council regularly engages with individuals in the community through advisory committees as well as formal community consultation programs and activities. Personal information provided by an individual as part of an advisory committee application or community consultation will be made available to Councillors and may be included in Council reports and working documents.

Personal information provided by an individual as part of a written public submission to a Council or committee meeting may be included in the published agenda and minutes of the meeting. These documents are displayed online and available in hardcopy format for an indefinite period of time.

Any individual who addresses a public Council or committee meeting will be heard and may be seen on the live stream. Any audio and video capture on the night will be recorded. Further information on the live streaming of Council meetings can be found in Council's Live Streaming and Publishing Recordings of Council Meetings Policy.

4.3 Principle 3 – Data Quality

Council must take reasonable steps to ensure that the personal information it collects, uses, or discloses, is accurate, complete, and up to date.

Accurate' means that the personal information is free from error or defect. If personal information used as the basis for Council decision is incorrect the resulting Council action may unintentionally cause harm to an individual or the community.

'Complete' means having all its parts or elements. It is important that all information is complete as partial information may be misleading to Council and result in an incorrect decision that may affect an individual or the community.

'Up to date' means extending to the present time; including the latest facts. This requirement is intended to deal with situations in which subsequent information would make the existing record inaccurate. It might not always be appropriate to delete the out-of-date information; the Public Records Act may require its retention. In these situations, it is best for Council staff to add a note detailing the information's lack of currency and add any new information.

Personal information must be accurate for the purpose it was collected. If the purpose has been completed and the records have been archived they no longer need to be monitored for data quality.

4.4 Principle 4 – Data Security

Council will take all necessary steps to ensure that personal information is stored safely and securely. This will ensure that all personal information held by Council is protected from misuse, loss and unauthorised modification and disclosure.

Personal information that a person provides to Council which is no longer necessary for Council purposes will be disposed of in accordance with the *Public Records Act 1973*.

4.5 Principle 5 – Openness

This document and Council's website details Council's management of personal information.

On request, Council will inform an individual, in general terms, of what information it holds on the individual, for what purpose this information is held and how the information is collected, held, used and disclosed. If the individual then requests further details, the individual can access their personal information held by Council as outlined in 'Access and Correction'.

4.6 Principle 6 – Access and Correction

Individuals have a right to ask for access to their personal information and seek corrections. Access will be provided except in the circumstances outlined in the Act, for example, where the information relates to legal proceedings, if it would pose a serious and imminent threat to life or health or impact the privacy of others.

Where a person requests Council to correct their personal information, Council will take reasonable steps to notify the person of the decision of the request as soon as practicable.

Personal information cannot be removed from records, but a correcting statement may be added.

As Council is subject to the *Freedom of Information Act 1982* (Vic) (FOIA), access to, or correction of personal affairs information is managed under that legislation. Under the FOIA, a person is also entitled to seek correction or amendment of a document containing their personal affairs information, where they believe the information is inaccurate, incomplete, out of date, or would give a misleading impression.

4.7 Principle 7 - Unique Identifiers

IPP7 provides a safeguard against the creation of a single identifier that could be used to cross match data across various government departments. Council will not assign, adopt, use, disclose, or require unique identifiers from persons except for the course of conducting normal Council business, or if required by law.

Council will only use or disclose unique identifiers assigned to a person by other organisations, if the person consents to the use and disclosure, or the conditions for use and disclosure as set out within the Act are satisfied.

4.8 Principle 8 - Anonymity

Where lawful and practicable, Council will give a person the option of remaining anonymous as part of his or her transaction with Council.

Before a member of Council staff collects personal information they must first establish whether that particular information is required to complete their function or activity.

Anonymity may limit Council's ability to process a complaint or other matter. Therefore, if a person chooses not to supply personal information that is necessary for the Council to perform its functions, then Council reserves the right to take no further action on that matter.

4.9 Principle 9 – Transborder Data Flows

The development of new technologies, such as the internet and the 'cloud' has meant that transborder data flows between organisations have become more common.

The transfer of personal information outside of Victoria is not prohibited. It is however, highly restricted to when it can occur. The basic premise behind IPP 9 is that when personal information subject to the Victorian legislation travels outside Victoria, the privacy protection in the Act should travel with it.

Council will only transfer personal information to an individual or organisation outside Victoria in the following circumstances:

- the individual has provided consent
- disclosure is authorised by law
- the recipient of the information is subject to a law, binding scheme or contract with similar principles as the Act; or
- the transfer is for the benefit of the individual and it is impracticable to obtain their consent before transfer however, it is apparent that they would likely provide consent to consent if it was practicable to obtain.

4.10 Principle 10 – Sensitive Information

Sensitive information is a subset of personal information. It is defined in the PDPA as *information or an opinion 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, membership of a trade union, sexual orientation or practices, criminal record*.

Council will not collect sensitive information about a person except in circumstances prescribed in the PDPA or in circumstances whereby such information is both directly pertinent and necessary to the specific, proper and legitimate functions of one or more of its activities.

4.11 Chief Privacy Officer

The Manager People and Performance is the Chief Privacy Officer responsible for:

- overseeing the implementation of the policy;
- monitoring the performance of the policy;
- reviewing the policy and recommending any desirable amendments; and

- periodically reporting to the Audit Committee on Council's performance pursuant to the policy.

4.12 How to Make a Complaint or Enquiry Concerning Privacy

Individuals who are concerned by Councils handling of their personal information are encouraged to contact the Chief Privacy Officer. The Chief Privacy Officer will then conduct a preliminary investigation and provide a written response within a reasonable timeframe. Complaints or enquiries to the Chief Privacy Officer should be sent to:

Manager People and Performance

PO Box 250

Nhill VIC 3418

Email: compliance@hindmarsh.vic.gov.au

Alternatively, complaints or enquiries may be made directly to the Office of the Victorian Information Commissioner. It should be noted that the Commissioner may decline to hear the complaint if the individual has not yet contacted Council with their concerns. ‘

Office of the Victorian Information Commissioner PO Box 24274

Melbourne VIC 3001

Email: enquiries@ovic.vic.gov.au

Website: www.ovic.vic.gov.au

Complaints must be lodged within 6 months of the time the complainant first became aware of the conduct or misconduct. At all times the contents of the complaint will be kept confidential.

Employees who are in breach of this policy may be subject to disciplinary action, performance management and review. Serious breaches may result in termination of employment, in accordance with Council's Disciplinary Guidelines.

4.13 Contract, MOU and Agreement Requirements

The following text outlines the minimum terms for Privacy provisions in contracts between Council and third parties.

i) The Recipient agrees that it is bound by the Information Privacy Principles and any applicable Code of Practice with respect to any act done, or practice engaged in, by the Recipient for the purposes of this Agreement in the same way and to the same extent as Council would have been bound by them in respect of that act or practice had it been directly done or engaged in by Council.

ii) Council may disclose to any person the fact that the Recipient is a party to this Agreement for the purpose of allowing such person to assess whether Transferred Personal Information is adequately protected in the hands of the Recipient. Council may also disclose a pro forma document containing terms substantially similar to the terms of this Agreement to any person for such purpose.

iii) The Recipient agrees that it will not at any time do an act, or engage in a practice, in respect of Transferred Personal Information, that would breach an Information Privacy Principle. Specifically the Recipient:

a) will not collect, use, disclose and otherwise handle the Transferred Personal Information for any purpose other than the primary purpose specified in this Agreement without the prior written permission of Council or the Data Subject or where required or authorised by or under Law;
b) will not disclose the Transferred Personal Information to a person (further recipient) who is not Council;
c) will take reasonable steps to ensure the security and quality of the Transferred Personal Information.

iv) The Recipient will immediately notify Council, in writing, of any breach or suspected breach of its obligations under this Agreement whether on the part of itself or its officers, employees, volunteers, agents or sub-contractors and of the steps taken to repair the breach.
v) The Recipient will allow and cooperate with any independent investigation of complaints by Council, OVIC or any person or body nominated by Council and provide appropriate redress to complaints for any harassing from it failure to effectively uphold the IPPs
vi) The Recipient at all times indemnifies and holds harmless Council from and against any loss, cost (including legal costs and expenses) or liability incurred or suffered by any of those indemnified arising from or in connection with any complaint, claim, suit, demand, action or proceeding by any person (including, but not limited to, any award, order or similar judgment or direction by the OVIC) where such loss or liability was caused or contributed to by the Recipient's act or omission in handling Transferred Personal Information, whether deliberate or not.
vii) Upon the termination of this Agreement, or upon the Council's written request prior to the termination of this Agreement, the Recipient will return or destroy Transferred Personal Information including all copies, in whatever form, of the Transferred Personal Information held or controlled by the Recipient.

5 References

Related documents	Legislation
Public Transparency Policy	*Privacy and Data Protection Act 2014* *Freedom of Information Act 1982* *Health Records Act 2001* *Victorian Charter of Human Rights and Responsibilities Act 2006* *Local Government Act 2020*

6 Document Control

Privacy and Data Protection Policy		**Policy Category**		Council
Version Number	1.1	**Policy Status**		Adopted
Approved/Adopted By	Council	**Approved/Adopted on:**		8 May 2024
Responsible Officer	CEO	**Review Date**		8 May 2027
Version History	**Date**	**Version**	**Description**	

	July 2009	1.0	New Policy
	December 2017	1.1	Update of Policy
	November 2018	1.2	Update of Policy – Formatting
	November 2020	1.3	Review of Policy – minor formatting changes. Inclusion of definitions and policy statement (Part 4)
	May 2024	1.4	Update of Policy – website information, collection statements, third party requirements, expansion of use and disclosure provisions.