POLICY POLICY POLICY POLICY

Macedon Ranges Shire Council

Policy Title:	**Privacy Policy**
Date of Adoption:	11 February 2020
Adoption Method:	☐ **Council** ☒ **Executive** ☐ **Other** ***(please specify)***
CEO Signature:	 **Date:** 6/3/20
Responsible Officer and Unit:	Coordinator Governance
Nominated Review Period:	☐ **Annually** ☒ **Other** ***(every 2 years)***
Next Review Date:	February 2022
References:	
Related Policies and Procedures:	Staff Code of Conduct Records Management Policy Disciplinary Policy and Procedure Electronic Visual Surveillance Policy and Procedure Information Security Policy
Related Resources:	Privacy Impact Assessment (PIA) template Interagency Request for Information template Privacy Data Breach template
Related Legislation:	*Privacy and Data Protection Act 2014 (Vic)* *Health Records Act 2001* (Vic) *Charter of Human Rights and Responsibilities Act 2006* (Vic) *Freedom of Information Act 1982* (Vic) *Public Records Act 1973* (Vic) *Surveillance Devices Act 1999* (Vic) *Telecommunications (Interception) (State Provisions) Act 1988* (Vic) *Victorian Protective Data Security Standards, Notifiable Conduct Scheme*

Contents

1. Purpose

To meet the requirements of the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001* regarding the management and handling of personal and health information.

The main purposes of these Acts are to:

- establish a system for the responsible collection, storage, handling and sharing of personal information
- inform individuals about how to access, correct, amend or transfer information about themselves which is held by council
- protect the privacy of an individual's health record that is held by Council.

2. Policy Statement

Macedon Ranges Shire Council is committed to protecting an individual's right to privacy. Accordingly, Council is committed to full compliance with its obligations under the *Privacy and Data Protection Act 2014*, the *Health Records Act 2001* and any other relevant legislation.

This policy is designed to help individuals understand how Council collects and manages personal information. Macedon Ranges Shire Council views the protection of an individual's privacy as an integral commitment to accountability and good governance.

3. Scope

This policy applies to both personal and health information held by Macedon Ranges Shire Council. This includes information Council has collected:

- from individuals, as well as information about individuals collected from third parties
- about individuals, regardless of format. This includes information collected on forms, in person, in correspondence (including emails and letters), over the telephone or via websites.

This policy applies to all Councillors, Council employees and contractors of Macedon Ranges Shire Council.

4. Definitions

4.1 Personal information

Information or an opinion, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

4.2 Sensitive information

Sensitive information is personal information that includes information or an opinion about an individual's, racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, criminal record, health or genetic information and/or some aspects of biometric information.

4.3 Health information

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

4.4 Health Services

An activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the organisation performing it to:

- assess, maintain or improve the individual's health
- diagnose the individual's illness, injury or disability
- treat the individual's illness, injury or disability or suspected illness, injury or disability
- provide a disability service, palliative care service or aged care service
- dispense a prescribed drug or medicinal preparation by a pharmacist
- provide a service, or class of service, provided in conjunction with an activity or service referred to above, which is a prescribed Health Service.

4.5 Information Privacy Principles (IPPs)

The ten principles established by the *Privacy and Data Protection Act 2014* that regulate how Council will collect, hold, manage, use, disclose or transfer personal information.

4.6 Health Privacy Principles (HPPs)

The eleven principles established by the *Health Records Act 2001* that regulate how Council as a health service provider will collect, hold, manage, use, disclose or transfer health information.

4.7 Public Registers

Documents that Council is required to make publicly available in accordance with legislation. Public registers may contain personal information and are open to inspection by members of the public. Examples of public registers maintained by Council include a register of building permits pursuant to section 31 of the *Building Act 1993* and a register of occupancy permits and temporary approvals received by Council pursuant to section 74 of the *Building Act 1993*.

4.8 Privacy Collection Notice

A statement that appears on Council's forms or registers that details why information is being collected by Council, to whom the information will/may be disclosed and why. It specifies any law that requires Council to collect the information and details how an individual can seek to gain access to the information they supply to amend it if required.

5. Principles

The 10 Information Privacy Principles (IPP) are:	The 11 Health Privacy Principles (HPP) are:
1. Collection	1. Collection
2. Use and Disclosure	2. Use and Disclosure
3. Data Quality	3. Data Quality
4. Data Security	4. Data Security
5. Openness	5. Openness
6. Access and Correction	6. Access and Correction
7. Unique Identifiers	7. Unique Identifiers
8. Anonymity	8. Anonymity
9. Trans-Border Data Flows	9. Trans-Border Data Flows
10. Sensitive Information	10. Transfer/closure of the Practice of a Health Service Provider
	11. Making information available to another Health Service Provider

Further information on the Information Privacy Principles is provided at **Appendix A.**

Further information on the Health Privacy Principles is provided at **Appendix B.**

Each of the principles and their correlation to the actions Council will undertake to deliver the requirements of the principles is outlined below.

5.1 Privacy Principle 1 – Collection

Council will only collect personal and/or health information that is necessary for carrying out its functions and activities. In some circumstances, Council is required by law to collect personal and/or health information.

If it is reasonable and practicable to do so, Council will collect personal and/or health information directly from individuals. When doing so, individuals will be informed of the matters set out in the legislation, including the purpose(s) for which the information is collected and will use lawful and fair means.

Council will take reasonable steps to make individuals aware of:

- who we are and how we can be contacted
- how individuals may gain access to the information
- the purpose/s for which information is being collected
- to whom Council discloses the information
- any relevant laws that require the information to be collected
- the main consequences (if any) for individuals if all or part of the information is not collected.

Where Council collects personal and/or health information about individuals from a third party, it will take reasonable steps (via at least one of the following methods - telephone, mail or email) to make those individuals aware of this, unless making them aware of the matter would pose a serious threat to the life or health of any individual.

Council Officers should complete a Privacy Impact Assessment (PIA) when collecting personal and /or health information for a new program or project, or when a program or project is being updated.

5.1.1 Collection notices

A privacy collection notice is to be included on all Council communications (hard copy and electronic) that collect personal and/or health information:

Privacy collection notice

Macedon Ranges Shire Council is committed to protecting your privacy. The personal information you provide on this form is being collected for the primary purpose of [reason for collecting the information].

Where required, [the personal information being collected, e.g. your identity*], will be provided to [people to whom the information will be provided, e.g.* Macedon Ranges Shire Council staff/contractors*] to enable them to [the reason/s they need the information, e.g.* process your application*].*

Your personal information will not be disclosed to any external party without your consent, unless required or authorised by law. If you wish to gain access to, or alter any personal information you have supplied on this [type of form, e.g. application / grant / agreement*], please contact us on [contact details].*

You can access Council's Privacy Policy at mrsc.vic.gov.au

5.2 Privacy Principle 2 – Use and disclosure

Council will use and disclose personal or health information about an individual for the primary purpose for which the information was collected. Council will also use or disclose information for a secondary purpose in other limited circumstances.

For example, Council may use or disclose information for law enforcement purposes to assist in the investigation of an unlawful activity that has been committed, being committed or in reporting concerns of the unlawful activity to the relevant authority.

Council may further use or disclose information where lawful to do so, including where necessary to lessen or prevent a threat to the life, health, safety or welfare of an individual or group.

5.3 Privacy Principle 3 – Data Quality

Council will take reasonable steps to ensure that all personal, sensitive and health information collected, held, used and disclosed is accurate, complete and up-to-date and relevant to its purpose, functions and activities.

5.4 Privacy Principle 4– Data Security and Retention

Council will take reasonable steps to maintain a secure system for storing personal and/or health information. Information systems and operational policies and procedures are in place to protect personal and/or health information from:

- misuse and loss
- unauthorised access, modification or disclosure.

Council regularly reviews its holdings of records (which can include personal information) and will destroy and transfer these records in accordance with its Records Management Policy and/or as required by law. Council will dispose of information where it is no longer necessary to fulfil the purposes for which the information was collected or as required by law.

All Council staff must comply with the *Public Records Act 1973* when disposing of Council documents. Officers are required to discuss the disposal of documents containing personal information with the Records Coordinator.

5.5 Privacy Principle 5 – Openness

This policy outlines Council's approaches to the management of personal and health information and is available on Macedon Ranges Shire Council's website or on request at Customer Service Centres.

On request, Council will inform an individual (where satisfied regarding that person's identity), 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.

5.6 Privacy Principle 6 – Access and Correction

Where Council holds personal or health information about a person, on request, it will provide that individual with access to that information unless one or more exemptions detailed in the *Privacy and Data Protection Act 2014* or the *Health Records Act 2001* applies.

Satisfaction of the conditions in these Acts could result in access being withheld in conjunction with an explanation of why the information is being withheld (for example where the information relates to legal proceedings or where the *Freedom of Information Act 1982* applies).

If an individual believes that their personal information and or health information is inaccurate, incomplete, or out of date, they may request Council correct and update the information. Requests to access and/or correct information will usually be formally handled under the *Freedom of Information Act 1982*.

5.7 Privacy Principle 7 – Unique Identifiers

Council does not assign, adopt, use, disclose or require unique identifiers (an identifier - usually a number – assigned to an individual uniquely to identify that individual for the purposes of the operations of the organisation) from individuals except in the course of conducting normal Council business or if required by law.

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

If an individual's contact details change, they are encouraged to contact Council so that the NAR database and other registers can be updated. Council conducts data matching periodically to ensure accurate name records are maintained on individual customers.

Council also maintains registers for other specific purposes e.g. mailing lists, customer lists, contact lists. These separate registers do not use unique identifiers.

5.8 Privacy Principle 8 – Anonymity

Where lawful and practicable, Council will provide individuals with the option of not identifying themselves when supplying information or entering into transactions with Council. Council will ensure individuals are aware of any limitations to services if the information requested is not provided.

5.9 Privacy Principle 9 – Trans-border data flows

Council will only transfer personal or health information outside of Victoria in accordance with the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*. For example, Council may transfer information about an individual where required by law; with consent of the individual; where the transfer is necessary for the performance or conclusion of a contract in the interest of the individual; and where reasonable steps have been taken to ensure the information transferred will not be held, used or disclosed by the recipient inconsistently with the privacy principles.

5.10 Privacy Principle 10 – Sensitive Information

Council will not collect sensitive information about an individual unless:

- the individual has consented
- the collection is required or authorised under law
- the collection is necessary to prevent or lessen a serious threat to the life or health of any individual
- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

Despite the conditions outlined above, Council may collect sensitive information about an individual if, for example, the collection:

- is necessary for research or the compilation or analysis of statistics
- is relevant to the provision of government-funded welfare or education services
- if there is no reasonably practicable alternative to collecting the information for that purpose (and it is impracticable to seek the individual's consent).

5.11 Health Privacy Principles 10 and 11 – Health service provider changes and information exchange

If Council discontinues the delivery of a Health Service, it will provide notice to past service users directly and by way of public notice in the local newspaper that the practice or business has been, or is about to be sold, transferred or closed down and the manner in which Council proposes to deal with the health information it holds.

If an individual requests Council, as a health service provider, to make health information available to another provider, Council will comply with that request as soon as practicable.

6. External contractors

While personal and/or health information is usually only handled by Council Officers, Council may outsource some of its functions to third parties e.g. a contractor (a person or body which provides service under a contract to Council). This may require the contractor to collect, use or disclose certain personal and/or health information (e.g. garbage collection and recycling, meals service). Contractors are contractually obliged to comply with the requirements of the legislation in all respects.

Council's contract agreements include the following statement regarding privacy:

> *The Contractor is bound by the Information Privacy Principles contained in the Privacy and Data Protection Act 2014 (Vic) in respect of any act done, or practice engaged in, by the Contractor for the purposes of this Agreement in the same way and to the same extent that Council would have been bound by them in respect of that act or practice had it been directly done or engaged in by Council.*

7. Closed Circuit Television (CCTV)

Council operates CCTV systems installed at fixed and mobile locations on land and buildings within the municipality. Council operates CCTV systems to support the provision and management of Council services, assets and facilities.

Data will only be collected, stored, accessed and disclosed in accordance with the *Privacy and Data Protection Act 2014*, the *Surveillance Devices Act 1999* and any other relevant legislation.

For more information, please refer to Council's Electronic Visual Surveillance Policy and Operating Procedure, available on the Council website.

8. Privacy Breaches and Complaints

Council Officers upon becoming aware that there has been a breach or potential breach of the Privacy Policy, will notify their supervisor without delay. The supervisor will follow the requirements of Council's Data Breach Response Plan.

If an individual is concerned about the management of their personal, health or confidential information, including any known or potential breaches they can make a complaint to Council's Privacy Officer:

Mail	Privacy Officer Macedon Ranges Shire Council PO Box 151 Kyneton Vic 3444
Telephone	03 5422 0333
Email	mrsc@mrsc.vic.gov.au

Complaints will be investigated and dealt with in accordance with Council's Complaints Handling Policy and Procedure.

Alternatively, individuals may make a complaint directly to:

Office of the Victorian Information Commissioner (OVIC)

PO Box 24274
Melbourne, Victoria 3001
Telephone: 1300 006 842

Email: enquiries@ovic.vic.gov.au

OR

Health Complaints Commissioner

Level 26
570 Bourke Street
Melbourne, Victoria 3000
Telephone: 1300 582 113

Note: These offices may decline to hear the complaint if the individual has not first made a complaint to Council.

Appendix A

Information Privacy Principles (IPPs)

Privacy and Data Protection Act 2014 (Vic)

No.	Principle		**Key Aspects** *(for the full and complete set of principles, refer to the Privacy and Data Protection Act 2014)*
1.	Collection	1.1	An organisation (including a person) must not collect personal information about an individual unless the information is necessary for one or more of its functions or activities
		1.2	An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
		1.3	At or near the time of collection, the organisation must notify the individual of a range of prescribed matters including the identity of the organisation, the purpose, proposed use and disclosure, right to access etc.
2.	Use and disclosure	2.1	An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless a prescribed exception applies
		2.2	If an organisation uses or discloses personal information under IPP 2.1(g) it must make a written note of the use or disclosure.
3.	Data quality	3.1	An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date
4.	Data security	4.1	An organisation must take reasonable steps to protect personal information it holds from misuse and loss and from unauthorised access, modification or disclosure
		4.2	An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose
5.	Openness	5.1	An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it
		5.2	On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information
6.	Access and correction	6.1	If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that prescribed exceptions apply
		6.5	If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete or up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date
7.	Unique identifiers	7.1	An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently
		7.2	An organisation must not adopt as its own identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless prescribed exceptions apply
8.	Anonymity	8.1	Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation
9.	Trans-border data flows	9.1	An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply
10.	Sensitive information	10.1	An organisation must not collect sensitive information about an individual unless the individual has consented or prescribed exceptions apply

Appendix B

Health Privacy Principles (HPPs)

Health Records Act 2001 (Vic)

No.	Principle		**Key Aspects** *(for the full and complete set of principles, refer to the Health Records Act 2001)*
1.	Collection	1.1 1.4	An organisation (including a person) must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and the individual has consented. At or near the time of collection, the organisation must notify the individual of a range of prescribed matters including the purpose, proposed use and disclosure, right to access etc.
2.	Use and disclosure	2.1 2.2	An organisation may use health or personal information about an individual only for the primary purpose for which the information was collected. An organisation must not use or disclose health information about an individual for a purpose other than the primary purpose unless the individual has consented to the use or disclosure
3.	Data quality	3.1	An organisation must take reasonable steps to make sure that the health information it collects, uses or discloses is accurate, complete and up to date and relevant to its functions
4.	Data security and retention	4.1 4.2	An organisation must take reasonable steps to protect the health information it holds from misuse and loss and from unauthorised access, modification or disclosure A health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate unless prescribed conditions apply
5.	Openness	5.1 5.2	An organisation must set out in a document its health information management policies, and access rights, and must make the document available to anyone who asks for it On request by an individual, an organisation must take reasonable steps to advise the individual about whether it holds their health information, how and why it is held, and the process for seeking access
6.	Access and correction	6.1 6.5	If an organisation holds health information about an individual, it must provide the individual with access to the information on request by the individual, unless prescribed conditions apply If an individual is able to establish that their information held by an organisation is inaccurate, incomplete, misleading or out of date, the organisation must take reasonable steps to correct the information
7.	Identifiers	7.1 7.2	An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently A private sector organisation may not adopt as its own identifier of an individual an identifier that has been assigned to that person by a public sector organisation unless prescribed exceptions apply
8.	Anonymity	8.1	Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation
9.	Trans-border data flows	9.1	An organisation may transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply
10.	Transfer or closure of the practice of a health service provider	10.1	If the practice or business of a health service provider is to be transferred or closed, the provider must comply with a prescribed set of procedures, including notification to former clients and the public
11.	Making information available to another provider	11.1	If an individual requests a health service provider to make their health information available to another provider, the former must comply with the request

Privacy Impact Assessment Template

A privacy impact assessment (**PIA**) is process for analysing a program's impact on individuals' information privacy. Undertaking a PIA can help to identify potential privacy risks, develop risk mitigation strategies, and enhance privacy practices when planning to collect personal information for new or revised programs and projects.

If your program involves the handling of personal information, it is best practice to conduct a PIA.

Undertaking a PIA is not just a compliance exercise – it is about improving organisational practice and demonstrating respect for individuals' privacy. The questions in this template go beyond the requirements under the Information Privacy Principles (**IPPs**) to encourage organisations to think about privacy and information management broadly, not just in the legal sense.

This PIA template has been prepared by the Office of the Victorian Information Commissioner (**OVIC**). It should be read alongside OVIC's Privacy Impact Assessment accompanying guide, which contains further information on how to complete this template.

Name of Program			
Name of Organisation	**Macedon Ranges Shire Council**		
Date		PIA Version Number	
PIA Drafter		Email	
Program Manager		Email	
Is your organisation a law enforcement agency as defined in section 3 of the *Privacy and Data Protection Act 2014*?			
Has the Privacy Officer of your organisation been consulted in the drafting of this PIA?			
Privacy Officer		Email	

Part 1 **Description of the program and parties**

[Delete the text below and add your description of the program and parties.]

This section should include:

- a detailed description of the program and its context;
- the purpose and objectives of the program;
- how the program will work;
- the expected benefits of the program and why it is necessary for your organisation's functions; and
- other parties (e.g. contracted service providers) and their roles, including the types of information they will be collecting and how they will use or disclose that information.

For more information, refer to section 1 in Part 1 of the accompanying guide (pages 10 – 11).

Scope of this privacy impact assessment

[Delete the text below and add your description of the PIA scope.]

This section should include:

- the elements of the program that this PIA process will and will not cover;
- any public interest determinations, temporary public interest determinations, information usage arrangements or certifications in place under the Privacy and Data Protection Act 2014 (PDP Act) related to this program;
- other PIA processes that have been undertaken that are relevant to this program; and
- where multiple parties are involved in a program, which party is covered in the PIA process.

For more information, refer to section 2 in Part 1 of the accompanying guide (pages 12 – 13).

Legal authority

[Delete the text below and add your description of your legal authority.]

This section should include:

- your organisation's legal authority to collect, use and disclose personal information for this program (under enabling legislation, the PDP Act or other legislation); and
- other legislation to consider when designing or implementing the program.

For more information, refer to section 3 in Part 1 of the accompanying guide (page 13).

Stakeholder consultation

[Delete the text below and add your description of your stakeholder consultation process.]

This section should include an:

- outline of any internal and external stakeholder consultation that has been undertaken in relation to the program; and
- where relevant, a summary of the outcomes of any consultation.

For more information, refer to section 4 in Part 1 of the accompanying guide (page 14).

Information flow diagram

[Delete the text below and insert your information flow diagram.]

Please insert below, or attach as an appendix, a diagram or table that shows the flow of information involved in this program, indicating the systems used and different parties involved (if applicable), and

the methods of transfer. Where possible, indicate the types of information that flow, between the various stages or parts of the program, and between different parties.

For more information, refer to section 5 in Part 1 of the accompanying guide (pages 14 – 15).

Part 2 **Privacy analysis table**

The following table assesses the privacy implications of your program. For guidance on responding to the questions, refer to the relevant section of the Privacy Impact Assessment Accompanying guide indicated in the last column.

Some questions in the table include prompts to assist you to identify privacy risks. However, you should think about potential privacy risks even when not explicitly prompted in the table and note any identified privacy risks in Part 3 of this template. You may also refer to the PIA guide for examples of potential privacy risks that may arise as you complete the privacy analysis.

Depending on your answer to a particular question, subsequent related questions may not be relevant or applicable. Where this is the case, please note this in your response.

Identifying information elements

#	*Question*	*Response*	*PIA guide*
1	**Does the program involve personal information?** *List each piece of personal information that is involved in the program.*		*6.2 – 6.5* *pp.16 – 17*
2	**Does the program involve other information that has the potential to identify individuals?** *This may include information that does not appear to be personal information at first glance, but which could identify individuals based on the context of the project or how the program uses the information.* *Describe this other information and explain how it could potentially identify individuals within the context of your program.*		*6.6* *p.17*
3	**Does the program involve sensitive information (as defined under Schedule 1 of the PDP Act)?** *Describe the type(s) of sensitive information that is involved in the program (if any), and how the collection or use of the sensitive information is authorised either by the PDP Act or other legislation.*		*6.7 – 6.9* *pp. 17 – 18,* *7.4* *p.20*
4	**Does the program involve health information?** *If the answer is yes, please refer to the Health Records Act 2001 or consult with the Health Complaints Commissioner in relation to health information (and where applicable, the Office of the Australian Information Commissioner).*		*6.10* *p.18*

5	**Does the program involve information that has previously been de-identified?** *Describe the type(s) of de-identified information that is involved in the program (if any), and the potential for re-identification.*		*6.13 – 6.18* *p.19*

Collection of personal information

6	**Is all the personal information collected necessary for the program?** *Explain why all the information collected is necessary for your program.*		*7.2 – 7.3* *p.20*

Privacy risk: If some personal information is not necessary for the program, consider whether there is a risk of over-collection.

7	**Do you need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?**		*7.5* *p.21*
8	**If individuals can remain anonymous, will you be collecting indirect identifiers, such as demographic information?**		*6.3 – 6.4* *p.17*

Method and notice of collection

9	**How will the personal information be collected?** *Describe the means by which the information will be collected. If personal information is collected via a third party platform, explain whether the platform will also be collecting that information*		*7.7 – 7.8* *p.21*

Privacy risk: Consider whether your method of collection is fair and not unreasonably intrusive.

10	**Is the personal information collected directly from the individual?**		*7.9* *p.21*
11	**Will the individual be notified about the collection of their personal information?** *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.*		*7.13 – 7.16* *p.22*

12	**Will any personal information about the individual be collected indirectly from another source?** *Describe how and from which other sources the personal information will be collected.*		*7.10 – 7.11 pp. 21 – 22*

Privacy risk: If you are collecting personal information indirectly, consider whether there is a risk of the information being inaccurate, out of date or incomplete. Consider the impact on individuals if they are not made aware that their information is being collected from another source.

13	**Will the individual be notified that their personal information has been collected from another source?** *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.*		*7.15 p.22*

Unique identifiers

14	**Will the program assign a unique identifier or collect a unique identifier assigned by another organisation to adopt as your organisation's own?** *Describe the unique identifier, the purpose for assigning or collecting it, and how this is authorised by either the PDP Act or other legislation.*		*7.18 – 7.19 p.23*
15	**Does the program require an individual to provide a unique identifier?** *Explain why or how the provision of a unique identifier is necessary for the program.*		*7.20 – 7.21 p.23*

Quality of personal information

16	**What steps will you take to ensure the personal information collected is accurate, complete, and up to date?**		*9.16 – 9.18 pp. 27 – 28*

Privacy risk: If there are inadequate or no steps taken, consider whether there is a risk that the information will be inaccurate, incomplete or out of date.

Security of personal information

17	**Are there security measures in place (existing or intended) to protect the personal information collected and used for this program?** *List the policies, procedures, or controls that your organisation implements to protect personal information. Please indicate how these measures will be governed. Include links or attachments where appropriate*		*8.2 – 8.9* *pp. 23 – 25*
18	**Where and how will personal information be stored?** *Describe the format in which the personal information will be stored (e.g. electronic, hard copy etc.) and where it will be stored (e.g. internally, external provider, cloud, third party platform etc.)*		*8.2 – 8.9* *pp. 23 – 25*
19	**Who will have access to the personal information?** *Describe the positions that will have access how access is gained or controlled, and whether it is logged.*		*8.2 – 8.9* *pp. 23 – 25*
20	**Have you completed a separate security risk assessment?** *If so, please refer to or attach a copy of the assessment to this PIA. If not, OVIC suggests you complete a security risk assessment.*		*8.10 – 8.11* *p.25*

Privacy risk: If there are inadequate or no security measures in place, consider whether there is a risk that the information will not be properly protected, leading to loss, misuse, or unauthorised access, modification or disclosure.

Primary and additional uses and disclosures of personal information

21	**Is the personal information (including any sensitive information) involved in this program used or disclosed for the main or primary purpose for which it was collected?** *Describe what personal information will be used or disclosed, and for what purposes.*		*9.2* *p.25*
22	**Does the program use or disclose personal information (including sensitive information) for a new or additional purpose other than the original purpose of collection?** *Describe the new/additional purpose for the use or disclosure of the information and explain how it is authorised, by either the PDP Act or other legislation. If relying on IPP 2.1(a), explain how the secondary use or disclosure is related to the primary purpose of collection.*		*9.3 – 9.4* *p.26*

Privacy risk: If relying on IPP 2.1(a) to use personal information for a secondary purpose, consider whether individuals would reasonably expect their information to be used for that secondary purpose. If relying on IPP 2.1(b) to use personal information for a secondary purpose, ensure the individual's consent is meaningful.

23	**Will the individual be notified of the additional use(s) of their personal information?** *Explain how the individual will be given notice of the secondary use(s) of their information, or why notice of the secondary use will not be provided.*		*9.4* *p.26*

Transfer and sharing of personal information

24	**Will any personal information be shared outside of your organisation?** *Describe:* • *what information will be shared;* • *with whom the information will be shared;* • *the frequency of the disclosure;* • *how the information will be shared; and* • *how the disclosure is authorised by either the PDP Act or other legislation.* *Identify whether any information sharing agreements are or will be in place, and how disclosures will be recorded.*		*9.6 – 9.7* *p.26*
25	*Describe what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred. Explain how the transfer is authorised by either the PDP Act or other legislation.*		*9.8 – 9.9* *p.26*

Other considerations relating to use and disclosure

26	**Does the program use or disclose a unique identifier assigned by another organisation?** *Describe the unique identifier and how it will be used or disclosed, and whether this is authorised by either the PDP Act or other legislation.*		*9.10 – 9.11* *p.27*
27	**Will any data matching occur as part of this program? This includes matching datasets within the program, or matching to other datasets external to the program.** *If so, explain the purpose for the data matching, what personal information will be matched and what other datasets it will be matched with, and what the combined dataset will be used for.*		*9.13 – 9.14* *p.27*
28	**Will any personal information be de-identified as part of the program?** *Describe the purpose for de-identifying personal information for the program, the method of de-identification, how the de-identified information will be used, and the potential for re-identification.*		*6.14 – 6.18* *p.19*

Privacy risk: If personal information is de-identified, consider whether there is a risk that the information can be re-identified. For example, de-identified information may be re-identifiable when matched to other information, or because of the way the de-identified information is used in the context of this program.

29	**How will you ensure the ongoing accuracy, completeness, and currency of the personal information used in this program?** *Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.*		*9.16 – 9.18* *pp. 27 – 28*

Management of personal information

30	**Is there a document available to the public that sets out your organisation's policies for the management of personal information, such as a privacy policy?** *Identify the document(s) and provide a link where available or include as an attachment to this PIA.*		*10.2, 10.5* *p.28*
31	**Will the document be updated to reflect the new collection or use of personal information for the purposes of this program?** *If not, explain why.*		*10.3* *p.28*
32	**Is there a way for a person to find out the types of personal information your organisation holds about them? Can you tell them the purposes for which it is held, and how your organisation collects, holds, uses and discloses that information?** *Describe the steps and provide links where relevant.*		*10.4 – 10.5* *p.28*

Access and correction of personal information

33	**How can individuals request access to, or correct their personal information?** *Identify the avenues available for individuals to request access to or correction of their personal information, and who is responsible for handling such requests.*		*10.6 – 10.7* *p.29*

Privacy risk: If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access and correction of personal information held by third parties. If not, there may be a risk that individuals cannot access or correct their personal information.

Retention and disposal of personal information

34	**How long will the personal information be kept for?** *Describe any relevant retention and disposal schedules or policies, including those issued by the Keeper of Public Records or those in other legislation.*		*11.2 – 11.3* *pp. 29 – 30*
35	**How will personal information be destroyed once it is no longer required?** *Describe the method of destruction and explain how that method is secure.*		*11.4* *p.30*
36	**As an alternative to destroying personal information, will any personal information be de-identified once it is no longer required?** *Describe the method of de-identification that will be used and the purposes to which the de-identified information will be put.*		*11.6 – 11.7* *p.30*
	Privacy risk: If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.		
37	**If applicable, what will happen to personal information held by third parties (such as contracted service providers, cloud storage, third party platforms etc.)?** *Describe any arrangements (for example, any contractual provisions) in relation to third parties' obligations to retain and dispose of personal information.*		*11.9 – 11.10* *pp. 30 – 31*
	Privacy risk: If there are no arrangements in place relating to third parties' retention and disposal of personal information, consider whether there is a risk that personal information will be held indefinitely.		

Other considerations

38	**Who can individuals complain to if they have concerns about the handling of their personal information?** *Identify the avenues (internal and external) for making a privacy complaint, including who is responsible for complaint handling.*		*12.2 – 12.4* *pp. 31*
39	**Does your organisation have a data breach response plan in place?** *If so, describe at a high level the steps that your organisation will take in the event of a data breach.*		*12.5 – 12.6* *pp. 31 –32*

40	**Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this program?** *Describe the type of training staff will receive.*		*12.7* *p.32*
41	**Will the program be evaluated against its objectives?** *Describe who will evaluate the program, at what point in the program evaluation will occur, and how often.*		*12.8* *p.32*
42	**Does the program comply with your organisation's other information handling or information management policies?**		*12.9* *p.32*
43	**Will this PIA be published?**		*p. 7*
44	**Are there any other broader privacy considerations associated with this program?**		*12.10* *p. 32*

Part 3 Risk Assessment Table

This section of the template lists any privacy risks that may have been identified during the privacy analysis in Part 2. The following table is a standard risk assessment template.

OVIC recommends that you use your organisation's own risk assessment framework where possible. (You may delete the table below and insert your own risk assessment table.)

For guidance on completing the risk assessment table, refer to sections 13 – 16 in Part 3 of the accompanying guide (pages 33 – 35).

#	Description of the risk	Impact rating	Likelihood rating	Risk rating	Accept risk (Y/N)	Risk management strategy	Residual impact rating	Residual likelihood rating	Residual risk rating	Risk owner
1	*'The risk of... event … caused by … how … resulting in … impact(s) …'*	*Rate the impact of the risk to your organisation.*	*Determine the likelihood of the risk occurring.*	*Assign an overall risk rating.*	*Identify whether your organisation will accept the risk or not.*	*Detail the measures taken (or to be taken) to mitigate and manage the risk. Where relevant, include the timeframe for implementing the strategy and identify who is responsible for it.*	*Rate the impact of the risk to your organisation after security measures have been applied.*	*Rate the likelihood of the risk occurring after security measures have been applied.*	*Assign an overall risk rating after security measures have been applied.*	*Assign a risk owner who will be responsible for monitoring and reviewing the risk.*
#										
#	*Insert additional rows as required*									

Summary of risks

[Delete the text below and add your summary of findings.]

This section should summarise the findings arising from the PIA process, including:

- Significant findings in relation to privacy risks, including any risks that cannot be mitigated. What is the likely public reaction to these risks? Are these risks outweighed by the public benefit that will be delivered by the program?
- Privacy enhancing features of the program.

For more information, refer to section 17 in Part 1 of the accompanying guide (page 36).

Part 4

The final section of this template covers any next steps that you may need to complete after undertaking the PIA process, endorsement of the PIA template or report, and document information. For more information refer to sections 18 – 22 in Part 4 of the accompanying guide (pages 33 – 38).

Action required

Where relevant, list the action items that need to be completed, who is responsible for that action, and any timeframes within which the action needs to be completed. These actions may be items that are identified during the privacy risk assessment, or over the course of undertaking the PIA process more broadly.

#	Action	Action Owner	Timeframe	Date Action completed

Endorsement

List any endorsements required for this PIA template or report. This may include the program manager or individual(s) with oversight over the program and privacy risks (if any), your organisation's Privacy Officer, and executive business owner.

Name	Position	Signature	Date

Document information

Document title	
Document owner	*Identify the branch, unit, team or individual within your organisation that has ownership over this document.*

Document distribution	*List any individuals or parties to whom this PIA template or report has been distributed. If your PIA template or report has been published, you may also include details of publication here (e.g. date of publication, website where published).*
Related documents	*List any other relevant documents that relate to this program, for example:* • *other relevant PIAs that have been undertaken (e.g. if this PIA only covers one aspect of the program)* • *security risk assessment* • *contract review* • *procurement requirements*

PIA review

Note when the PIA template or report will be reviewed to ensure that it is still accurate. If required, the PIA template or report should be updated to account for any changes to the program.

Date review should be completed by	

Document version

Version number	Date	Document status	Author
		e.g. 'draft' or 'final'	

ABN 42 686 389 537

PO BOX 151 KYNETON VIC 3444
T 03 5422 0333
F 03 5422 3623
E: mrsc@mrsc.vic.gov.au
www.mrsc.vic.gov.au

Inter-agency Information Request

To be completed by agencies requesting access to personal and/or health information held by Macedon Ranges Shire Council (MRSC) and emailed to mrsc@mrsc.vic.gov.au

Agency and officer details	
Date:	Reference number:
Agency/Authority:	Business Unit:
Requesting officer :	Position/Authority:
Telephone:	Email:
Address:	
Information requested (please provide specific details)	
Reason and legislative authority for request: include relevant legislative breaches under investigation and/or before the courts that the information is relevant to.	
Outline why the information is reasonably necessary, including the agency's legislative authority to make the request and the relevant Information Privacy Principle (IPP) of the Privacy and Data Protection Act 2014	
Applicable law / legislation:	Applicable offence(s):

Declaration

For the protection of information, the requesting body gives the following assurances to meet the obligations of the *Privacy and Data Protection Act* 2014 *(Vic):*

- No document or information derived from any document given under this request will be disclosed to another person unless required by compulsion of law (eg subpoena), authorised by law enforcement agency/ officer
- Physical versions or copies of documents given under this request will be stored in a secure facility that is physically protected against unauthorised access including the use of lockable containers, cabinets, and restricted access rooms.
- Electronic versions or copies of documents given under this request will be appropriately protected against unauthorised access including the use of passwords, encryptions, firewalls, and other appropriate protections.
- Adequate security measures will be implemented to protect all documents given under this request during storage, handling and transport including when contained on portable computing devices or portable data storage devices.
- Physical and electronic versions or copies of any document given under this request will be securely destroyed or permanently de-identified when the information is no longer required.
- Macedon Ranges Shire Council will be immediately advised if any document given under this request is to be disclosed to any person (including under the Freedom of Information Act) or is disclosed without proper authority or is relevant to any complaint or legal proceeding.

Signature of requesting officer:	**Date:**

Macedon Ranges Shire Council

Response to request (Internal use only)

Assessment of request	
Council officer's name:	**Position / business unit:**
Decision (*full/partial/declined):*	**Relevant document numbers:**
Date of release:	**Method of release:**
Rationale for decision:	
Information provided: (additional attached as required)	

MRSC assessment guidelines/checklist:

1. Check that the entity making the request is a legitimate agency / law enforcement body.
2. You must have a reasonable belief that disclosure is required. You should be able to present evidence to justify this belief. Ideally, you should require any request for information to be made in writing.
3. Finally, your belief must be that the information is reasonably necessary for the operation of the agency / law enforcement related activity. This is an objective test as to whether a reasonable person, properly informed, would agree to disclosure in your circumstances. Again, you should be able to justify why this is the case, and the best chance to do this is to ensure sufficient information is provided by the requesting body to allow the general nature of the matter to be understood

Privacy Data Breach Template

Purpose

The purpose of the Privacy Data Breach Template is to set out processes for Council in the event that Council experiences an information breach (or suspects that an information breach has occurred).

Scope

This policy applies to all people with access to Council's information systems and records (computer based or otherwise) including Council officers, volunteers, work experience placements, trainees and independent contractors and consultants.

What is a data breach?

A data breach occurs when information held by Council is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

Data breaches may arise from:

- loss or unauthorised access, modification, use or disclosure or other misuse;
- malicious actions, such as theft or 'hacking';
- internal errors or failure to follow information handling policies that cause accidental loss or disclosure; and
- not adhering to the laws of the states and territories or the Commonwealth of Australia.

Responding to Data Breaches

When a Council employee or contractor becomes aware or suspects that there has been a data breach, they will notify their immediate line manager who will assess the risk, document the event and generate the report of the incident as required in Attachment A.

Council's GOVERNANCE TEAM should be provided with a completed copy of this form as standard practice and will retain a repository of all breach incidents.

Attachment A – Privacy Data Breach Template

The following template is based on the questions outlined by the Office of the Victorian Information Commissioner (OVIC).

More information on responding to privacy breaches is available online at WWW.OVIC.VIC.GOV.AU

The Governance team can provide advice on completing this form and whether it is necessary to notify OVIC.

Description	Details	
Provide a short description of the breach, including the date and time that the breach was discovered and the duration and location of the breach.		
Date of breach		
Brief description		
Date breach identified		
How the breach was identified		
Location of breach		
Cause of the breach		
Step 1 - Breach Containment and Preliminary Assessment		
Have you contained the breach (recovery of information, computer system shut down, locks changed)? • *Have you designated an appropriate individual to lead an initial investigation of the breach?* • *Have you determined who needs to be made aware of the incident internally and externally?* • *Do internal parties such as Governance, Building Maintenance, Customer Service, and Information Services been notified?* • *Do external parties such as insurers, other agencies, professional or regulatory bodies, financial institutions or contractors need to be notified?* • *Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?*		
Responsible individual for Investigation	**Name:**	**Title**:
Remedial action taken to contain breach		
Who needs to be made aware of the breach?	**Internal:**	
	External:	

Step 2 – Evaluate Risks Associated with the Breach	
What personal information was involved?	
What was the cause and extent of the breach?	
How many individuals are affected and who are they?	
What is the foreseeable harm from the breach?	
Step 3 – Notification	
Should affected individuals be notified? • *What are the reasonable expectations of the individuals concerned?* • *What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?* • *Is there a risk of physical harm? Is there a risk of embarrassment, humiliation or damage to the individual's reputation?* • *What is the ability of the individual to avoid or mitigate possible harm?* • *What are the legal and contractual obligations of the organisation?* • *Is notification likely to cause more harm to the individual?*	
If affected individuals are to be notified, when and how will they be notified and who will notify them?	
What will be included in the notification? *Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:* • *information about the incident and its timing in general terms;* • *a description of the personal information involved in the breach;* • *a general account of what your organisation has done to control or reduce the harm;* • *what your organisation will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves;* • *sources of information designed to assist individuals in protecting against identity theft;* • *contact information of a department or individual within your organisation who can answer questions or provide further information;* • *whether your organisation has notified the Victorian Information Commissioner;* • *additional contact information to address any privacy concerns to your organisation; and* • *contact information for the Office of the Victorian Information Commissioner.*	
Step 4 – Prevention of Future Breaches	
What short and/or long-term steps do you need to take to correct the situation (e.g. staff training, policy review or development, improved security measures, audit of information handling, including record retention)?	**Short-term:** **Long-term**: