INFORMATION PRIVACY POLICY

Policy No.	C22	Adoption Date:	Council Meeting 13 December 2023
Revision Date:	December 2027		
Directorate:	Performance & Innovation	Department:	Digital & Technology
GOOD GOVERNANCE FRAMEWORK – OVERARCHING PRINCIPLES			
Supporting Pillar:	Pillar 7 - Risk & Compliance		
Link to Pillar:	The Information Privacy Policy supports the "Risk & Compliance" pillar by outlining the responsibilities that Council must adhere to, to protect personal and private information.		

1. PURPOSE

1.1. The purpose of the *Information Privacy Policy* (C22) (the Policy) is to explain:

1.1.1. How Council collects, holds, uses and discloses personal, health, and sensitive information of individuals;

1.1.2. How individuals can gain access to their information and correct inaccuracies; and,

1.1.3. How individuals can submit a complaint about possible breaches of privacy.

1.2. Council is strongly committed to protecting every individual's right to privacy.

1.3. The Policy also aims to protect the personal information of people collected by Council.

1.4. This Policy has been developed to ensure compliance with the *Privacy and Data Protection Act 2014* and the *Information Privacy Principles* identified in the Act.

2. SCOPE

2.1. The scope of this Policy applies to anyone whom Council collects, uses or discloses personal information about. This includes information about Ratepayers / Residents / visitors, Council staff, Councillors, contractors and volunteers. This also includes Council's website and Social Media sites.

Collection and Management of Personal Information

2.2. This Policy applies to the collection, use, storage, transfer, handling, right of access, and amendment of personal information at Council.

2.3. The following may not apply, but should be consulted on:

2.3.1. Personal information which is maintained on a public register;

2.3.2. Information recorded in a de-identified way which cannot be linked (or re-linked) to a known individual;

2.3.3. Personal information which is already available in a publication or other publicly available document; or

2.3.4. Information which is generally available.

3. POLICY PRINCIPLES

Overarching Governance Principles of the *Privacy and Data Protection Act 2014*

3.1. The *Privacy and Data Protection Act 2014 (the Act)* applies to all public sector organisations operating in Victoria, including South Gippsland Shire Council. The Act dictates how Council is required to handle personal information and the conditions in which it must be collected, managed and destroyed.

3.2. The Act refers to a set of principles, known as the Information Privacy Principles (IPPs) that specify how Council is required to handle personal information at each point of its lifecycle. These IPPs are:

Principle 1 – Collection

Principle 2 – Use and Disclosure

Principle 3 – Data Quality

Principle 4 – Data Security

Principle 5 – Openness

Principle 6 – Access and Correction

Principle 7 – Unique Identifiers

Principle 8 – Anonymity

Principle 9 – Transborder Data Flows

Principle 10 – Sensitive Information

3.3. Council has implemented, and will continue to implement, reasonable measures to ensure compliance with the Act.

Applicability

3.4. Councillors, Council staff, contractors and volunteers must adhere to the *Information Privacy Principles* as dictated by the *Privacy and Data Protection Act 2014 (the Act)*.

3.5. Councillors are subject to this Policy as members of Council and as individual public officials. Consequently, Councillors must deal with personal information in compliance with this policy's principles, and do not have unrestricted access to personal information held by Council, nor do they have an unrestricted right to use and disclose such information.

3.6. Contractors who are working for Council, and with access to Council resources, information, data, and technology are responsible for adhering to this policy and *The Act*, the extent and nature of which must be identified in their contract or agreement.

3.6.1. Where appropriate, contractors must also undergo privacy training upon commencement of their work, and every 12 months there-after.

3.7. Personal information is defined under the Act, as information or an opinion that is recorded in any form, whether true or not, where identity can be reasonably ascertained.

Collection

3.1. Council will only collect personal information that is necessary for the performance of its functions. Sometimes, this information collection is required by law. Council will also ensure that it only collects sensitive information where consent is obtained, or such collection is permitted under the Act.

3.2. A collection statement must be made available for individuals to inform them who is collecting their information, why their information is being collected, whether it is required by law, how an individual can gain access to the information and what the consequences may be if an individual fails to provide that information.

3.3. Where possible, Council will endeavour to collect information directly from the individual.

3.4. This principle applies to Councillors who consequently must only collect personal information that is necessary for them to carry out their functions as Councillors.

Use and Disclosure

3.5. Council will only use and disclose personal or sensitive information where:

3.5.1. It is in accordance with the primary purpose it was collected for;

3.5.2. Where explicit and express consent is granted for the use or disclosure to Third parties; and,

3.5.3. In accordance with provisions made within the Act (e.g., a secondary purpose in which a person would reasonably expect, where it is required by law to disclose etc.).

3.6. Access to information will always be on a 'need to know basis'.

Data Quality

3.7. Council will take reasonable steps to ensure individuals' personal information is accurate, complete and up to date.

3.8. Reasonable steps will also be taken to ensure that personal information is not kept longer than required under relevant laws or acts.

Access and Security of Personal Information

3.9. Council will take reasonable steps to protect individuals' personal information from misuse, loss, unauthorised access, modification or disclosures.

3.10. When conducting Council business from outside of Council premises, care needs to be taken to keep personal or sensitive information secure.

3.11. Council will maintain data security and protection in accordance with the *Victorian Data Protection Security Standards V2.0* (VPDSS 2.0) as set out in sections 86, 87 and 88 of the Act.

Openness

3.12. Council will ensure openness and integrity by ensuring this policy will be made accessible to anyone who requests it, including members of the public.

3.13. Council will ensure this Policy is publicly available via Council's main website and links through social media pages.

Access, Correction and De-Identifying

3.14. In most cases, Council will facilitate requests to access private information under the *Freedom of Information Act 1982,* in acknowledgement of an individual's right to seek access to their personal information and make corrections.

3.15. This is subject to some limitations or exceptions, including where:

3.15.1. Access would pose a threat to the life or health of an individual, or

3.15.2. A document is classified as exempt from the *Freedom of Information Act 1982*.

3.16. All personal information will either be de-identified or destroyed at the end of its lifecycle, or when it is no longer legally required.

Automatic processing of data, cookies, and similar technologies

3.17. Council may process information including personal information and conduct automated decision-making and reporting.

3.18. Council may collect personal and other information using cookies. Cookies allow a website to store information on a machine or mobile device and retrieve it later. Some cookies are managed by Council, while others are managed by third parties the not controlled by Council (third-party cookies), such as Google.

3.19. Individuals may choose not to accept cookies in connection with use of Council websites and online services by deleting, blocking or disabling cookies via your browser setting.

Unique Identifiers

3.20. Council will not adopt or share unique identifiers (i.e. a number or other code associated with an individual's name, such as a driver's license number).

3.21. The exception to this is where such circumstances deem the adoption of a unique identifier is necessary to carry out Council functions or is exempt under the *Privacy and Data Protection Act 2014.*

Anonymity

3.22. Individuals will be given the option of not identifying themselves when they engage with Council, as long as it is lawful and feasible.

3.23. Individuals need to be aware that anonymity may prevent Council from taking appropriate action, resolving an issue or providing a response to the individual.

Trans-border Data Flows

3.24. There may be circumstances where Council will transfer personal or health information (other than Council or the individual), to an entity who is outside Victoria, but only in the following instances:

3.24.1. If consent is provided, or consent may be reasonable inferred; or

3.24.2. If the transfer is for your benefit, it is impractical to obtain your consent and if it were practical to obtain that consent, you would be likely to give it; or

3.24.3. The transfer is necessary for the performance of a contract between the individual and the organisation; or

3.24.4. If disclosure is authorised and required by law; or

3.24.5. If Council has taken reasonable steps to ensure data will not be handled inconsistently with the Information Privacy Principles; or

3.24.6. If the recipient of the information is subject to a law, binding scheme, or contract with similar Principles as the *Privacy and Data Protection Act 2014*.

Sensitive Information

3.25. Council will not collect sensitive information except in circumstances described by the *Privacy and Data Protection Act 2014* or in circumstances where the information is both directly pertinent and necessary to one of its functions.

3.26. Sensitive information includes information about an individual's race or ethical origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.

Privacy Notification

3.27. On all forms and documents (including electronic forms), which collect personal information, Council will include a privacy collection statement that is endorsed and approved by Council's appointed Privacy Officer.

3.28. The collection statements will include who is collecting their information, why their information is being collected, whether it is required by law, how an individual can gain access to the information, and what the consequences may be if an individual fails to provide that information.

3.29. Council will also automatically include in all e-mails that are sent to non-Council e-mail address external to Council, the following disclaimer for the purposes of protecting personal information and Council's intellectual property:

> *This email and any attachments may contain information that is personal, confidential, copyright and/or subject to legal and other professional privilege. No part of it should be reproduced, adapted or communicated without the prior written consent of the copyright owner. You must not use, disclose or act on the email in any way if you are not the intended recipient of the information. The confidentiality and privilege are not waived or lost by reason of any mistaken transmission. South Gippsland Shire Council collects, uses and discloses your personal information in accordance with the Council's Information Privacy Policy at www.southgippsland.vic.gov.au*

The Privacy and Data Protection Act (the Act) and Other Laws

3.30. Council understands and acknowledges that section 6 of the *Privacy and Data Protection Act 2014* states that if a provision of the Act is inconsistent with another Act, including the *Local Government Act 2020*, the other Act prevails.

3.30.1. This may lead to the legitimate disclosure of personal information outside the *Privacy and Data Protection Act 2014*.

Website Privacy Statement

3.31. In addition to privacy collection statements being included on all collection points, Council will also include a Privacy Statement on its website. This statement will include an individual's right, avenues for access, change or privacy breaches, and links to this Policy.

Privacy Breaches

3.32. In the event that data has or is thought to be misused, has unauthorised access, modification or disclosure, individuals may reach out to Council's Privacy Officer to request an investigation.

3.32.1. Council's Privacy Officer can be contacted via post at:
Att: Privacy Officer
9 Smith Street
Leongatha VIC 3953

3.32.2. Alternatively, the Privacy Officer can be contacted via email to council@southgippsland.vic.gov.au

3.33. If Council finds a breach has happened, contact will be made to the affected individuals to let them know of the breach, and steps moving forward.

3.34. All investigations are reported through Council's Privacy and Cybersecurity Board and breaches will be reported to Office of the Victorian Information Commissioner (OVIC).

3.35. If an individual is unsatisfied with Council's response to an investigation or breach, they can contact OVIC via email at enquiries@ovic.vic.gov.au.

4. RISK ASSESSMENT

This Policy mitigates Council's risks as described below:

People

4.1. This Policy aims to provide a clear understanding of how personal information is collected and handled in line with the *Privacy and Data Protection Act 2014*.

Reputational

4.2. This Policy helps mitigate potential reputational risk due to inappropriate collection, usage or sharing of personal information.

Financial

4.3. This Policy helps prevent possible financial risk due to breaches of privacy according to the Act.

Governance

4.4. This Policy refers to and outlines relevant legislation that governs the collection, use and access of personal or sensitive information. See section 8 for a list of these legislations.

5. IMPLEMENTATION STATEMENT

Human Rights Charter

5.1. This Policy has considered the *Charter of Human Rights and Responsibilities Act 2006* in its development.

Gender Equality

5.2. This Policy has considered the *Gender Equality Act 2020* in its development.

Roles and Responsibilities

5.3. The Policy will be published on Council website.

5.4. Privacy training will be conducted for new and current staff.

5.5. The Chief Executive Officer appoints the Coordinator Information Compliance & Data Integrity as Council's Privacy Officer. This position will be responsible for managing matters in this policy, privacy complaints and privacy statements.

Non-compliance with this Policy

5.6. Non-compliance with this Policy will result in an investigation into the matter. Action may result in the form of training and education to disciplinary action, depending on the results of the investigation.

6. MONITORING, EVALUATION AND REVIEW

6.1. This Policy will be reviewed and adopted by Council on a four-year cycle.

7. REFERENCE DOCUMENTS

Legislative Provisions	Charter of Human Rights and Responsibilities Act 2006 Freedom of Information Act 1982 Health Records Act 2001 Local Government Act 1989 Local Government Act 2020 Privacy and Data Protection Act 2014 Privacy Act 1988
Council Supporting Documents	Information Technology Strategy

8. DEFINITIONS

Personal Information	Information or an opinion that has been recorded in any form where the identity of an individual from such information could be reasonably ascertained. The information can be true or false. Personal Information which falls under the *Health Records Act 2001* is not included as part of the *Privacy and Data Protection Act 2014.*
Information Privacy Principles (IPPs)	A list of Principles set out in Schedule 1 of the Privacy and Data Protection Act 2014. The IPPs outline how to handle personal information throughout its lifecycle.
Collection Statement	A statement that outlines what is formation is being collected, by who, why, how the information will be managed and what consequences may result if an individual refuse to provide information.
Sensitive information	Sensitive information is information about a living individual's race or ethnicity, political opinions, religious or philosophical beliefs, sexual preferences or practices, criminal record, or membership details, such as trade union or professional, political or trade associations.
Health information	Health information is information about a living or deceased individual's physical, mental or psychological health.

9. REVISION HISTORY

Approved By	Approval Date	Sections Modified	CM9 Ref#
Council	*22 May 2013*	*Policy Review*	*D8200714*
Council	*27 September 2017*	*Policy Review*	*D6006317*
Council	*25 November 2020*	*Policy Review*	*D9306620*
Council	*13 December 2023*	*Policy Review*	*D37524*