Privacy Policy

Policy statement

Gippsland Water values and respects the privacy of personal and health information.

We ensure that all personal information is collected, used, disclosed and stored lawfully and securely.

Purpose

This policy establishes the principles governing how we manage personal and health information. It ensures we:

- Handle personal and health information transparently and lawfully
- Protect individuals' privacy rights
- Promote an ethical culture within Gippsland Water in relation to privacy and information handling
- Provide clarity on what information is collected, how it is handled and used, and how it is protected
- Ensure all Board members, employees and contractors are aware of their responsibilities in relation to managing personal and health information
- Meet our legislative obligations, including those relating to personal payment information under PCI-DSS.

Scope

This policy applies to all Board members, employees and third-party contractors of Gippsland Water (we).

It covers personal and health information (personal information) relating to customers, consumers, employees and others (you).

It also applies to personal payment information (credit card information) handled on our behalf by PCI-DSS compliant service providers.

Policy details

Compliance with the *Privacy and Data Protection Act 2014* (Vic)

- We will use, disclose and hold the personal information we collect in accordance with the *Privacy and Data Protection Act 2014*, in particular, the Information Privacy Principles.
- Where health information is collected by us, we will handle that information in accordance with the *Health Records Act 2001* (Vic).
- We will actively comply with these and any other applicable law and standard to protect and maintain privacy of your personal information, including (where applicable) the *Privacy Act 1988* (Cth), and the Notifiable Data Breaches Scheme.

Collection

- We collect and handle personal information because of our role in providing:
    - Water and wastewater services including access to assets we own and manage to maintain and complete works in accordance with the *Water Act 1989* (Vic)
    - Our land, reserves, facilities and catchments within our region
    - Our commercial services, through Gippsland Regional Organics, and Gippsland Agribusiness
    - Employment of people to deliver our services
    - Engagement of organisations and individuals to delivery our services.
- We will only collect personal information that is necessary to perform our functions and activities, including the information needed to manage or administer them.
- We may receive health information for the provision of our services, or in the course of receiving the details of an enquiry or a complaint. Health information of our staff may also be collected from time to time, for example, in the course of approving personal leave.
- Where reasonably practicable, we will collect information directly from you. Information can also be lawfully provided by government agencies and departments, employees and other third parties, such as real estate agents, authorised representatives or through notices of acquisition or disposition. Where reasonably practicable, we will notify you when information about you has been collected from third parties.

- When collecting personal information from an individual, we will take reasonable steps to advise you of:
    - what information is being sought
    - for what purpose(s) it is being collected
    - whether any law requires the collection of the information
    - how you can contact us
    - the main consequences, if any, of not providing the information.
- As far as is practicable, we will inform you of how we intend to use your personal or health information and who your information may be disclosed to.

Use and Disclosure

- We will only access personal information to the extent necessary to perform our roles.
- We use or disclose personal information only for:
    - the primary purpose of collection
    - a related secondary use reasonably anticipated by you
    - a purpose to which you have consented
    - a purpose authorised or required by law, which may include emergency situations, assisting law enforcement agencies, or disclosures to credit reporting bodies for debt recovery purposes.
- We may disclose personal information to our service providers who support the delivery of our services. Such disclosures are made on a confidential basis and subject to contractual obligations requiring appropriate privacy and security protections, including PCI-DSS compliance where applicable.
- Information may be held in hard copy or electronic form, or as voice or video recordings. Our obligation to hold in confidence all information of a personal nature is not diminished regardless of the way in which it is collected.
- We will not otherwise use or disclose personal or health information unless permitted by law.

Data quality

- We will take reasonable steps to ensure personal information is accurate, complete and up to date. Where possible, we will check the accuracy of personal or health information with you before using it.

Data security and retention

- We will take reasonable steps to protect personal information we hold from misuse, loss, unauthorised access, modification or disclosure through appropriate physical, technical and administrative measures.
- Information is destroyed or permanently de-identified when it is no longer required in accordance with the *Public Records Act 1973* (Vic) and the relevant Retention and Disposal Authorities.

Privacy Impact Assessments

- We will actively review and assess our privacy risks with any new project, system, process, initiative or significant change that involves personal information or where personal information is handled, through a privacy impact assessment (PIA) process.
- PIAs must be completed during early planning to identify privacy risks, ensure legislative compliance, and embed privacy-by-design.
- Any decision not to complete a PIA must be documented and approved, with justification recorded.

Personal Payment Information (PCI-DSS)

- We recognise the sensitivity of personal payment information (credit card details) and ensure all handling complies with the Payment Card Industry Data Security Standard (PCI-DSS).
- Where we offer credit card payment options, this is handled exclusively through PCI-DSS compliant systems and third-party providers.
- We do not store, process or transmit cardholder data internally.

Openness

- We make information about our privacy policy and practices available through our website, published materials and collection notices.

Access and correction

- We will provide you with reasonable access to your personal information held by us and will take reasonable steps to correct such information when requested by you, in order to ensure that our records are accurate.
- We will endeavour to maintain accurate records. When an error is identified (either internally or by an external party) we will correct the information promptly.
- We will take steps to verify the identity of any individual who requests access to, or correction of, their information held by us before considering the request.
- Requests for access to and/or correction of documents containing personal information held by us will be handled in accordance with the *Freedom of Information Act 1982* (Vic) and should be addressed in writing to:

  Email: privacy@gippswater.com.au

  Post: Privacy Officer, Gippsland Water, 55 Hazelwood Road, Traralgon, VIC, 3844

Unique identifiers

- We will not assign unique identifiers to individuals unless it is necessary to enable us to carry out our functions efficiently.
- We will not request a unique identifier created by another organisation unless required by law, or use or disclose a unique identifier created by another organisation unless there is a lawful basis for doing so.

Anonymity

- When seeking general information from us, you do not have to identify yourself. If you make a general enquiry, no personal information will be collected or recorded unless we need this information to get back to you with an answer to your enquiry.
- However, to provide services such as water or wastewater services, personal information is required. In most cases this will be provided by you directly, but in some situations it may be supplied to us by authorised third parties (e.g. through property-related legal notices or managing agents).
- In limited circumstances where safety-related risks exist, additional protections may be applied to how personal information is handled or disclosed.

Transfer of information outside Victoria

- Information will not be transferred outside Victoria unless permitted by law, subject to appropriate safeguards, or you provide your consent (which may be implied in some cases).
- Any other transfers of information outside Victoria will be made in accordance with the *Privacy and Data Protection Act 2014* (Vic).
- We may engage third-party online service providers (for example, email newsletter services and survey tools), that store personal information outside Australia. Where you choose to use these services, you may consent to this transfer, and the information will be handled in accordance with the third-party providers privacy policy.

Complaints about privacy

- If you wish to make a privacy complaint against us, you can do so by contacting the Privacy Officer:

  Phone: 1800 050 500

  Email: privacy@gippswater.com.au

  Post: Privacy Officer, Gippsland Water, 55 Hazelwood Road, Traralgon, VIC, 3844

- We treat complaints seriously and will try to resolve them fairly and quickly. If you make a complaint, we will work with you to resolve your complaint and keep you informed of its progress.
- Alternatively, you may make a complaint to the Victorian Information Commissioner or the Health Complaints Commissioner (although the Commissioner may decline to hear the complaint if you have not first made a complaint to us).

  Victorian Information Commissioner

  Phone: 1300 006 842

  Email: enquiries@ovic.vic.gov.au

  Health Complaints Commissioner

  Phone: 1300 582 113

  Email: hcc@hcc.vic.gov.au

Data Breaches

- Where a data breach involves payment card data handled by a PCI-DSS compliant provider, we will follow the incident response and notification requirements agreed with that provider, including any obligations to notify the provider, relevant card schemes and affected individuals.
- Where a privacy breach relates to personal information regulated under Victorian legislation, we will comply with any notification or reporting requirements issued by the Office of the Victorian Information Commissioner.

Notifiable Data Breaches Scheme

- We will comply with the requirements of the Notifiable Data Breaches Scheme, which requires us to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals if an eligible data breach has occurred involving Tax File Number information.
- An eligible data breach occurs if each of the following applies:
    - There is unauthorised access to or unauthorised disclosure of personal information or loss of personal information (where this is likely to result in unauthorised access or unauthorised disclosure)
    - A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the affected individuals
    - We have not been able to prevent the likely risk of serious harm occurring with remedial action.
- A failure to notify the OAIC of an eligible data breach is deemed an interference with privacy and may trigger the Australian Information Commissioner's enforcement powers under the *Privacy Act 1988* (Cth).

Roles and Responsibilities

Board	The Board is responsible for: • Demonstrating leadership and promoting an organisation wide 'privacy culture'. • Ensuring that this policy is consistent with our strategic direction and any other policy. • Approving any amendment to this policy.

- Notifying the Privacy Officer of any suspected or confirmed privacy breach in a timely manner.

Executive Leadership Team	The Managing Director and the Executive Leadership Team are responsible for: • Demonstrating leadership and promoting an organisation wide 'privacy culture'. • Monitoring, reviewing, and recommending approval of policies and practices to ensure they remain relevant and effective. • Establishing governance mechanisms for privacy responsibilities. • Notifying the Privacy Officer of any suspected or confirmed privacy breach in a timely manner.
Managers and Leaders	Managers are responsible for ensuring that: • They demonstrate leadership and promote an organisation wide 'privacy culture'. • Privacy policies and practices are operationalised within their workgroup, including the use of appropriate collection statements, security controls and ensuring that necessary privacy and PCI-DSS controls are built into new systems that handle personal or payment card information. • The Privacy Officer is notified of any suspected or confirmed privacy or payment card data breach in a timely manner. • Responses to requests from the Privacy Officer are timely and transparent manner to assist with any complaint or suspected/confirmed privacy breach. • Privacy Impact Assessments are completed for any new project, process review or initiative that involves personal information or impacts on information management practices or processes within their remit. • The Information asset register for their workgroup is maintained, including the type of personal and financial information used or held and how it is secured.

- Staff are supported to participate in regular privacy and information security awareness training and activities, including any training required to meet PCI-DSS obligations.

Privacy Officer	The Privacy Officer is responsible for: • Providing internal privacy advice. • Coordinating the response to any suspected or confirmed privacy breaches, including those involving payment card data. • Handling privacy complaints that we receive directly. • Promoting privacy awareness and activities for staff. • Liaising with relevant privacy regulators. • Assessing whether requests from other organisations to share personal information that we hold are permitted under privacy law.
Employees, Contractors	Employees and Contractors are responsible for: • Adhering to the requirements outlined in this Policy. • Ensuring responses to requests from the Privacy Officer are completed in a timely and transparent manner. • Participating in Privacy Impact Assessments for any new project, process review or initiative that involves personal information or impacts on information management practices or processes within their work area. • Actively participate in regular privacy awareness training and activities, and where relevant, PCI-DSS awareness training and activities. • Notifying the Privacy Officer of any suspected or confirmed privacy or payment card data breach in a timely manner.

Definitions

Credit Card payment	Any payment received by Gippsland Water made with any Mastercard or Visa credit or debit card.
Commissioner	The Victorian Commissioner for Privacy and Data Protection.
Contracted service provider/Third party contractor/Contractors	A person or body in the capacity of a contracted service provider, including any subcontractor engaged for the purposes (whether direct or indirect) of a contract.
Gippsland Water	Central Gippsland Region Water Corporation (ABN 75 830 750 413) and its related entities.
Health information	Personal information or an opinion about a living or deceased individual's physical, mental or psychological health, disability, expressed wishes about the future provision of health services, or access to health services as defined in the *Health Records Act 2001*.
Location of personal Information	Gippsland Water holds personal information if the information is contained in a document in our possession or under our control, whether alone or jointly with other persons or bodies, irrespective of where the document is situated.
Payment Card Industry Security Council	The organisation established by the payment card industry to improve the security of credit card information.
Payment Card Industry Data Security Standard (PCI-DSS)	The standard produced by the Payment Card Industry Security Council that must be complied with as a minimum to ensure the security of customer credit card information.
Personal information	Information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, but does not include information to which the *Health Records Act 2001* (Vic) applies.
Privacy legislation	The *Privacy and Data Protection Act 2014* (Vic).

Privacy Officer	The Gippsland Water staff member delegated with the responsibilities as described in this Policy.
Sensitive Information	Personal information (including an opinion) about an individual: • 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 preferences or practices • criminal record.
Unique Identifier	An identifier (usually a number) assigned to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name, and does not include an identifier within the meaning of the *Health Records Act 2001* (Vic).

Policy review and approval

Minor administrative changes that do not materially alter this policy may be made without approval. Examples include template updates, job title changes or minor legislative updates without material impact.

Responsible Officer	Review Frequency	Approving Body
Governance Leader	Every four years	Board

References

Related legislation

1. Privacy Act 1988 (Cth)

2. Privacy and Data Protection Act 2014 (Vic)
3. Charter of Human Rights and Responsibilities Act 2006 (Vic)
4. Freedom of Information Act 1982 (Vic)
5. Gender Equality Act 2020 (Vic)
6. Public Records Act 1973 (Vic)
7. Surveillance Devices Act 1999 (Vic)
8. Victorian Data Sharing Act 2017 (Vic)
9. Water Act 1989 (Vic)

Related policies and frameworks

- Victorian Protective Data Security Framework (VPDSF)
- Payment Card Industry Data Security Standard (PCI-DSS)
- VPSC Code of Conduct for Directors
- VPSC Code of Conduct for Employees
- Closed Circuit Television (CCTV) Policy
- Risk Management Policy
- Records Management Policy
- Acceptable use policy for Information, Communication & Technology (ICT) Resources Policy
- Security Policy
- Business Continuity Policy
- Family Violence Policy – Employees
- Family Violence Policy – Customers
- Generative Artificial Intelligence Policy

Related guidelines – Office of the Victorian Information Commissioner

- Information Privacy Principle Guidelines

- Collection notices
- Privacy impact assessments
- Use of enterprise Generative AI tools in the Victorian public sector
- Use of personal information with publicly available Generative AI tools in the Victorian public sector
- Artificial Intelligence – Understanding Privacy Obligations