

Internal Privacy Policy

Approved

21 October 2025

1. PURPOSE

Respect for privacy is important for gaining and retaining the trust and confidence of our customers, our people and the communities in which we operate. At Meridian Energy Limited (Meridian) we are committed to dealing with the information of our customers, people and stakeholders in ways that are consistent with the Privacy Act 2020 (Act).

2. SCOPE

This Policy **provides a framework** that promotes an understanding of our privacy obligations and sets robust processes when handling personal information to ensure we comply with the Act.

It **applies to all Meridian employees and suppliers** who have access to personal information and other business information in relation to our operations, employees and customers (both residential and business).

This Internal Policy must be read in conjunction with Meridian's **Careers Privacy Policy, Record Management Policy, Information Security Policy, Information Classification and Protection Policy** and Meridian's **Code of Conduct**.

3. MERIDIAN'S PRIVACY VISION

Our **privacy vision** outlines Meridian's commitment to protecting the privacy of individuals and maintaining their trust in Meridian. We continually monitor and evolve our privacy practices to meet the evolving privacy landscape in New Zealand and to ensure the privacy rights of our stakeholders are upheld.

Our vision is:

- **Legal Compliance:** We comply with all privacy laws in New Zealand. We will regularly review and update our practices to align with any changes in legislation.
- **Collection and Consent:** We are transparent in our data collection practices, clearly explaining the purpose and scope of data collection to individuals. Consent to the collection, use or disclosure of personal information will be obtained in a clear, understandable, and accessible way.
- **Data Security:** We implement reasonable and robust security measures to protect personal information from unauthorised access, disclosure, alteration, or destruction. We will also educate our employees about data security best practices.

- **Data Minimisation and Retention:** We only collect personal information that is necessary for the purpose for which it is being collected. We will retain personal information only where there is a legitimate business purpose for doing so or as required by law. When no longer needed, we will securely dispose of or anonymise personal information.
- **Rights and Access:** We respect the rights of individuals regarding their personal information. This includes providing individuals with access to their personal information upon request, allowing them to correct inaccuracies, and giving them the option to opt out of certain data processing activities, where applicable.
- **Third-Party Data Sharing:** We will establish clear agreements and procedures for data sharing, ensuring that appropriate safeguards are in place to protect personal information.
- **Training and Awareness:** We provide privacy training and awareness programs to our employees to ensure they understand their responsibilities and obligations regarding privacy protection.
- **Governance and Accountability:** We have clear lines of accountability (via Privacy Champions, and our Privacy Officer) for overseeing privacy-related matters within Meridian. The Privacy Officer or their delegate will monitor and report on compliance, respond to privacy-related queries, and handle privacy breaches or incidents promptly and transparently.
- **Privacy Culture and Continuous Improvement:** We foster a culture that values privacy and embeds privacy considerations into our decision-making processes and business practices. We will regularly review and enhance our privacy strategy and practices, taking into account technological advancements, industry standards, and feedback from stakeholders.

4. RESPONSIBILITIES

- **Privacy Officer**

The Act requires Meridian to appoint a Privacy Officer who is responsible for, amongst other things, being familiar with Meridian's obligations under the Act, working to make sure Meridian complies with the Act, acting as Meridian's liaison with the Office of the Privacy Commissioner, reporting to the Meridian Board on any privacy related issues. The General Counsel is Meridian's designated Privacy Officer. The Privacy Officer may delegate certain aspects of their role.

- **Business Unit Privacy Champions**

Business unit Privacy Champions have been appointed as the contact persons within their business unit to assist the Privacy Officer to ensure that Meridian complies with its obligations under the Act, including managing privacy-related incidents within their business unit. Privacy Champions for each Business Unit can change. You can see who the Privacy Officer and the Business Unit Privacy Champions are on **Electric Avenue** if you have any privacy-related questions or concerns.

5. EMPLOYMENT PRIVACY OBLIGATIONS

The **Meridian and Powershop Careers Privacy Policies** sets out what we do and how we will comply with our obligations under the Act when you apply to become, or are, an employee of Meridian, including:

- the kinds of personal information that we collect and hold about you;
- how and when your personal information is collected, disclosed and used by us;
- the purposes for which we collect, hold, use and disclose personal information; and
- how you may access your personal information and seek correction of your personal information.

6. PRIVACY PROCESSES

All Meridian employees and suppliers who have access to personal information in relation to our operations, employees or customers are expected to understand and comply with the requirements of the Act and the other relevant Meridian policies and guidelines relating to the confidentiality and protection of personal information.

Meridian has developed the following principles and processes to support its compliance with the Act. For the avoidance of doubt the following principles and processes are applicable to all employees and suppliers and are in addition to the minimum requirements set out in the Act.

	Policy principle	Process
1.	Information Privacy Principles The Act has 13 Information Privacy Principles that govern how Meridian should collect, handle and use personal information.	• You are expected to comply with the Information Privacy Principles when you collect, use or store personal information. You can read more about these Information Privacy Principles here.
2.	Collection of personal information Personal information can only be collected for a lawful purpose connected to a Meridian activity – for example, obtaining personal information when onboarding a new customer, working with a new supplier, or working through the recruitment process	• When asking for personal information, think carefully about why you are collecting it and don't collect personal information unless it is necessary for that purpose. • Personal information should be collected directly from the person it is about, unless the person has authorised collection from someone else, the personal information is otherwise publicly available or another exception in the Act applies.

	with a potential employee.	
3.	Storage, security and disposal of personal information Meridian's Code of Conduct requires all Meridian employees to maintain and protect the confidentiality of personal information entrusted to or generated by Meridian. Under the Information Privacy Principles, Meridian is also required to ensure there are safeguards in place to prevent the loss, misuse or disclosure of personal information.	• Our Information Security Policy and Information Classification and Handling Policy provides a set of principles and procedures that business units and our people are required to follow to ensure that information security risk management is taken into consideration and should be read in conjunction with this Policy. • Our Records Management Policy sets out the minimum and/or maximum time frames for which we must retain personal information. For customer personal information, Meridian only retains that information for so long as it is required by law or for a legitimate business purpose (e.g., knowing who our customers are in the event we need to correct their bill in future).
4.	Use of personal information Meridian will not use personal information for any reason other than for which it was collected.	• Personal information may only be accessed, used or disclosed for genuine business purposes . • Personal information stored or held by Meridian may only be accessed by authorised personnel. • Our Information Classification and Handling Policy set out these requirements for accessing, using and disclosing personal information.
5.	Access to and correction of personal information Our customers and employees have a right to ask for access to and correct (if required) their personal information that is held by Meridian.	• If someone requests a copy of their personal information or requests to change/correct the personal information we have for them, you must deal with those requests in accordance with the Information Privacy Principles and provide the information in a clear and convenient form.
6.	Disclosure of personal information Meridian will not disclose personal information to any third party without consent of the	• We require an individual's consent before we share their personal information. • We expect our employees who have and use personal information to take appropriate steps to share only the minimum of what is needed or requested and ensure the security of that information (including when sharing that

	individual involved, or where such disclosure is required by law.	information internally and externally), which includes appropriate storage and may include encrypting and password protecting any personal information. • In some situations, there may be a reason to refuse a request for access to personal information (for example, the information may involve an unwarranted breach of someone else's privacy or releasing the information may pose a serious threat to someone's safety). If you have any concerns with providing access to personal information, please talk to the People Team or Legal Team, as appropriate, in the first instance. • Personal information may only be disclosed to an organisation outside New Zealand if the individual has consented to their personal information being shared, or other criteria required under the Act are met. If you intend to disclose personal information to a recipient outside New Zealand or enter into a contract that permits the disclosure of personal information outside New Zealand, you must contact the Legal Team to ensure that Meridian can comply with its obligations under the Act. • From time-to-time Meridian may receive a request for access to personal information from a specific agency (e.g., NZ Police, Inland Revenue Department, Immigration NZ, Ministry of Social Development). No personal information should be released to any agency without following the processes approved by the Legal Team or without first speaking to the Retail Compliance Manager or the Legal Team. • If a customer or employee requests for Meridian to delete any personal information that is held about them, please talk to your Business Unit Privacy Champion and/or the Legal team. • Meridian will take reasonable steps to ensure that the personal information it holds is accurate, up to date, complete and not misleading.
7.	Privacy breaches A privacy breach occurs when someone intentionally or accidentally breaches one of the 13 Information Privacy Principles, for example providing unauthorised access	• All employees are expected to report any actual or suspected privacy breaches such as an unauthorised disclosure of someone's personal information to the Retail Compliance Manager or Legal Team as soon as possible. If you are in the Retail Team, this includes completing a Privacy Breach form. • The Legal Team should be informed of privacy breaches in accordance with the timeframes set out in the Compliance Policy and Compliance

	to someone's personal information, or inadvertently disclosing, altering, losing or destroying someone's personal information.	Policy Process. The Legal Team will use the guidelines provided by the Privacy Commissioner to determine next steps. • Meridian has reporting obligations to the Privacy Commissioner in respect of serious privacy breaches, so it is important that all privacy breaches are reported as soon as possible. • If a privacy breach has occurred, details of the breach are to be reported in the monthly Compliance Report. • If a person is impacted by a privacy breach, Meridian's approach is to proactively advise that person of the breach (unless there is a reason to do otherwise). You must consult with the Legal team if you intend to discuss an actual or suspected privacy breach with a person impacted by a privacy breach; or take other corrective action in relation to that privacy breach.
8.	Training	We expect all employees who have access to, use or collect personal information held by Meridian to complete any required training modules as soon as possible after joining us, so that they understand their obligations, and refresh that training annually.
9.	Related documents	The following policies and process documents are relevant to Meridian's compliance with the Act: • Meridian and Powershop Privacy Policies • Meridian and Powershop Website Terms of Use • Meridian and Powershop Career Privacy Statements • Meridian Code of Conduct • Records Management Policy • Information Classification and Protection Policy • Information Security Policy