Munro Benge
Chartered Accountants Limited

PRIVACY POLICY

How Munro Benge collects, uses, protects and shares personal information

Document Number	MB-101-V01
Approval Date	September 2026
Approved by	Management Team
Review Cycle	At least annually and on any material change to PS-2 or applicable law

Contents

1. About this policy

Munro Benge Chartered Accountants Limited (Munro Benge, we, us or our) is committed to protecting personal information. This policy explains how we collect, hold, use, disclose and protect personal information and how individuals may exercise their rights.

This policy applies to personal information about clients, prospective clients, client representatives and beneficial owners, suppliers, website visitors, job applicants and other people who interact with us. Separate internal policies may apply to employees and contractors.

We comply with the Privacy Act 2020, including the information privacy principles, and any other applicable legal, regulatory, contractual and professional obligations. Nothing in this policy limits an individual's rights under law.

2. What personal information we collect

The information we collect depends on our relationship with the individual and the services involved. It may include:

- **Identity information.** Names, dates of birth, signatures, photographs, copies of identity documents, citizenship or residency details, and information about directors, trustees, shareholders, partners and beneficial owners.
- **Contact information.** Addresses, email addresses, telephone numbers and communication preferences.
- **Tax and government identifiers.** IRD numbers, ACC information, Companies Office details and other identifiers needed for an engagement or required by law.
- **Financial and business information.** Bank-account details, transactions, income, expenses, assets, liabilities, ownership, payroll, accounting records and other financial or commercial information.
- **Engagement and communication records.** Agreements, instructions, correspondence, meeting notes, service history, complaints and records of our interactions.
- **Compliance information.** Identity-verification, source-of-funds or source-of-wealth information, sanctions or politically exposed person checks, and information needed to meet anti-money-laundering, countering-financing-of-terrorism, tax or professional obligations.
- **Technical and website information.** IP address, device or browser information, website activity and information collected through cookies or similar technologies.
- **Recruitment or supplier information.** Qualifications, employment history, references, background information, payment details and other information relevant to the relationship.

Some records may contain information about other people. A person who gives us another individual's information must have authority to do so and should make this policy available to that individual where appropriate.

3. How we collect personal information

We usually collect information directly from the individual through meetings, email, telephone, forms, our website, secure portals, engagement documents and material supplied for our services.

We may also collect information from authorised representatives; employers or associated entities; Inland Revenue, ACC, the Companies Office and other public bodies; banks, lawyers, advisers and former accountants; identity-verification and credit-reporting providers; publicly available sources; and other third parties where collection is authorised, required or otherwise permitted by law.

> **INDIRECT COLLECTION:** Where Information Privacy Principle 3A applies, we will take reasonable steps, as soon as reasonably practicable after collection, to tell the individual that information has been collected from another source, why it was collected, its intended recipients, who collects and holds it, any relevant statutory authority, and the individual's access and correction rights—unless an exception applies.

We collect personal information only where it is necessary for a lawful purpose connected with our functions or activities, and we seek to collect it by lawful, fair and reasonably non-intrusive means.

4. Why we collect and use personal information

We may collect and use personal information to:

- assess enquiries, establish and manage engagements and communicate with clients and their representatives;
- provide accounting, taxation, advisory, compliance, payroll, company-secretarial and related services;
- prepare, review, file or deliver financial statements, returns, reports, applications and other documents;
- verify identity, authority and beneficial ownership and conduct conflict, fraud, sanctions and other compliance checks;
- meet obligations under tax, company, anti-money-laundering, employment, privacy and other laws and professional standards;
- obtain information from, and communicate with, Inland Revenue, ACC, banks, regulators and other authorised parties;
- manage billing, credit, debt recovery, supplier relationships, insurance, quality control and business administration;
- maintain, secure, improve and audit our systems, services and records;
- respond to questions, complaints, access or correction requests, disputes, investigations and legal processes;
- recruit personnel and manage professional or commercial relationships; and
- send newsletters or marketing where permitted, with an option to unsubscribe from electronic marketing.

We will not use personal information for a materially different purpose unless that use is authorised by the individual, is directly related to the original purpose, or is otherwise permitted or required by law.

5. When providing information is optional or required

Unless we explain otherwise, providing information is generally voluntary. However, some information is required by law, by an engagement, or for us to provide services safely and effectively. If required information is not provided, we may be unable to accept or continue an engagement, complete work, communicate effectively, meet a deadline or comply with legal and professional duties.

6. Accuracy and minimisation

We take reasonable steps to collect only information that is relevant and necessary. Before using or disclosing personal information, particularly where it may affect an individual, we take reasonable steps to ensure it is accurate, up to date, complete, relevant and not misleading. Individuals should tell us when their information changes or appears incorrect.

7. Who we may disclose information to

We may disclose personal information where reasonably necessary for the purposes described in this policy, where authorised by the relevant individual or client, or where permitted or required by law. Recipients may include:

- Inland Revenue, ACC, the Companies Office, regulators, courts, Police and other government or law-enforcement agencies;
- banks, insurers, lawyers, auditors, actuaries, valuers and other professional advisers involved in an engagement;
- authorised reviewers and professional bodies, including reviewers appointed for professional-practice or quality reviews and bound by confidentiality obligations;
- Walker Wayland group members and other specialists engaged to assist with authorised work;
- technology, cloud, document-signing, identity-verification, accounting, payroll, communications, storage, support and other service providers that process information for us;
- debt-collection, credit-reporting or dispute-resolution providers where appropriate;
- a purchaser, successor or adviser involved in a proposed or completed business reorganisation or transfer, subject to appropriate safeguards; and

- any other person authorised by the individual or the relevant client.

We do not sell personal information. Service providers may use information only to provide authorised services or as otherwise permitted by their contract and applicable law. We take reasonable steps to select providers with appropriate privacy, confidentiality and security safeguards.

8. Overseas storage, processing and disclosure

Some service providers, including cloud and software providers, may store or process personal information outside New Zealand or allow authorised support access from overseas. Where a provider stores or processes information solely as our agent, we remain responsible for that information as required by the Privacy Act.

If we disclose personal information to a foreign person or entity for its own purposes, we will comply with Information Privacy Principle 12. This may include confirming comparable privacy safeguards, using appropriate contractual protections, or obtaining express authorisation after explaining that comparable safeguards may not apply.

9. How we protect personal information

We use safeguards that are reasonable in the circumstances to protect personal information against loss, misuse, unauthorised access, disclosure, alteration and destruction. Safeguards may include:

- role-based access, strong authentication and access reviews;
- secure devices, networks, backups, transmission and approved cloud services;
- confidentiality obligations, staff training and acceptable-use requirements;
- physical security for offices and paper records;
- vendor due diligence, contractual controls and incident-management procedures; and
- secure disposal or de-identification when information is no longer required.

No method of storage or transmission is completely secure. We review and improve safeguards in proportion to the sensitivity of the information and the risks involved.

10. Retention and disposal

We retain personal information only for as long as it is needed for the purpose for which it was collected, to provide services, resolve issues, maintain appropriate professional records, or meet legal, tax, anti-money-laundering, insurance and contractual requirements. Retention periods vary by record type. When information is no longer required, we securely delete, destroy or de-identify it, subject to lawful holds and backup-management processes.

11. Artificial intelligence and automated tools

We may use approved technology, including artificial-intelligence-assisted tools, to support administrative, analytical or drafting tasks. Personal or confidential information may be processed only through approved systems and for authorised purposes, with appropriate privacy, security and contractual safeguards. Material outputs are subject to appropriate human review. We do not rely solely on automated processing to make a decision with significant effects on an individual unless the use is lawful, appropriately assessed and subject to meaningful human oversight.

12. Website, cookies and social media

Our website may collect technical information and use cookies or similar technologies to operate, secure and understand use of the site. Browser settings may allow cookies to be limited or blocked, although some features may not function properly.

We use third-party social-media services. If an individual communicates with us through those services, the platform may collect and use information under its own privacy terms. Social-media platforms do not receive access to personal information held in our internal systems merely because an individual interacts with our page.

Our website may link to third-party sites. We are not responsible for their privacy practices and recommend reviewing their privacy notices.

13. Accessing and correcting personal information

An individual may ask us to confirm whether we hold personal information about them and request access to or correction of that information. Requests may be made using the contact details below. We may need to verify identity and authority before responding.

We will respond as soon as reasonably practicable and no later than 20 working days, subject to any lawful extension. The Privacy Act permits information to be withheld in some circumstances. If we decline an access or correction request, we will explain the applicable reason and available complaint rights. If we do not make a requested correction, the individual may ask us to attach a statement of correction to the information.

14. Privacy breaches

PLEASE TELL US PROMPTLY: If personal information has been sent to the wrong person, lost, accessed without authority or otherwise compromised, contact our Privacy Officer immediately so we can contain and assess the incident.

We investigate suspected privacy breaches and take steps to reduce harm. Where a breach has caused, or is likely to cause, serious harm, we will notify the Office of the Privacy Commissioner and affected individuals as soon as practicable, unless a statutory exception applies. We aim to assess potential notifiable breaches promptly, taking account of the Commissioner’s expectation that notification should ordinarily occur within 72 hours of awareness.

15. Questions and complaints

Questions, access or correction requests, and privacy complaints should be directed to:

Privacy Officer: Munro Benge Chartered Accountants Limited

Address: Level 3, 104 The Terrace, Wellington 6011; PO Box 1400, Wellington 6140

Telephone: 04 472 7465

Email: munrobenge@munrobenge.co.nz

Website: www.munrobenge.co.nz

We will try to resolve privacy concerns promptly and fairly. If an individual is not satisfied with our response, they may complain to the Office of the Privacy Commissioner at www.privacy.org.nz or telephone 0800 803 909.

16. Changes to this policy

We may update this policy to reflect changes in law, technology, services or business practices. The current version will be made available through our usual publication channels and will show its effective date. Material changes will be communicated where appropriate.