

1 PURPOSE

Privacy Policy current as at October 2026.

We know that how we collect, use, disclose and protect your information is important to you, and we value your trust. That's why protecting your information and being clear about what we do with it is a vital part of our relationship with you.

The purpose of this Privacy Policy is to inform our clients and users of our digital platforms (including our website, Facebook, Messenger, Instagram, WhatsApp, WeChat and other communication channels we may use) about how we comply with the New Zealand Privacy Act 2020 (the Privacy Act) when managing personal information.

2 CONSENT TO PRIVACY POLICY

By engaging us, using our digital platforms or providing personal information to us, you acknowledge this Privacy Policy and authorise us to collect, use, store and disclose information as described in it, subject to the Privacy Act 2020 and your rights under that Act.

3 COLLECTION OF PERSONAL INFORMATION

Personal Information is defined in the Privacy Act as information about an identifiable individual (a natural person as opposed to a company or other legal entity).

3.1 TYPES OF PERSONAL INFORMATION WE COLLECT

The types of personal information we collect will vary depending on the nature of your dealings with us. We only collect personal information that is necessary. Where reasonable and practicable, we will collect your personal information directly from you and inform you that we are collecting it.

We mainly collect personal information directly from you, for example:

- Over the telephone or a video call (including Google Meet, Microsoft Teams, Zoom or similar platforms), for example when you contact our staff;
- Through one of our digital platforms, such as our website, Facebook, Messenger, Instagram, WhatsApp or WeChat (including through online chat, virtual assistants or bots);
- When you email or write to us; or
- When you participate in a marketing campaign, competition or promotion (or a similar event) administered by us or our representatives.

If it is not obvious that we are collecting personal information from you, we will do our best to make it clear to you so that you are always aware when information is being collected.

Generally, the types of personal information we collect and hold include your:

- Name
- Date of birth
- Contact details (such as your email address, postal address, phone number)
- Details relating to your use of any product and/or service offered by us
- Details of your enquiry
- Details of any preferences you tell us about (such as subscription preferences).

We may also collect personal information about you from:

- Publicly available sources e.g., via the internet.
- Your professional advisers, such as sharebroker, lawyer and banker etc.;

Where we collect personal information about you from someone other than you, we will do so only where permitted by the Privacy Act 2020 or another law. We will take reasonable steps to notify you of the indirect collection and the matters required by Information Privacy Principle 3A as soon as reasonably practicable, unless an exception applies or you have already been made aware. We are not responsible for the privacy or security practices of the source from which the information was obtained.

3.2 ONLINE DEVICE INFORMATION AND COOKIES

If you visit our website or interact with our digital or social-media platforms, information about your use and experience may be collected through cookies, pixels, software development kits and similar technologies used by us or the relevant platform provider. These technologies can record information about your visit or interaction so that the service can function, remember preferences, provide analytics and improve the user experience.

Cookies and similar technologies are controlled by the relevant website or platform and operate within the permissions of your browser, device and platform settings. Third-party platforms may also use their own cookies or similar technologies in accordance with their privacy policies.

When you interact with us through our website or another digital platform, information collected through cookies or similar technologies may include:

- The date and time of visits;
- Website page (or pages) viewed;
- The website, application or platform from which you accessed our website or other digital platform;

- How you navigate through the website and interact with pages (including any fields completed in forms and applications completed (where applicable));
- Information about your location;
- Information about the device used to visit our digital platform; and
- IP address (or addresses), and the type of web browser used.

We will not ask you to supply sensitive personal or financial information publicly through Facebook, Messenger, Instagram, WhatsApp, WeChat or any other social-media or messaging platform that we use. We may invite you to send limited details by private message, for example to answer an enquiry, but where sensitive accounting, tax, banking or identity information is required we may direct you to a more appropriate or secure channel.

3.3 BOTS AND ARTIFICIAL INTELLIGENCE

We may use bots, workflow automation and artificial-intelligence tools to assist with enquiries, administration, drafting, summarisation, research, document review and other professional-support activities. If you interact with an automated feature through our website or a third-party platform, information you provide may be processed by the relevant platform provider and, where applicable, by Wix as our website platform provider so that the feature can operate.

The relevant platform or AI provider may retain or process information in accordance with its own privacy and service terms. We apply professional judgement and internal controls when deciding what information is appropriate to provide to automated or AI tools. We recommend that sensitive personal, tax, banking or identity information is not provided through a public bot or social-media chat unless we specifically request it and consider that channel appropriate.

4 PURPOSE OF COLLECTION AND USE OF PERSONAL INFORMATION

Any personal information you provide to us may be used to:

- Check whether you are eligible for the product or services offered by us;
- Facilitate those services;
- Provide information that you request; and / or
- Provide you with further information about our other products and services.

We also have an obligation to maintain personal information to disclose to regulatory and similar bodies - see "[Disclosure of your personal information](#)" below. These bodies have a legal right to such information.

5 STORAGE AND PROTECTION OF YOUR PERSONAL INFORMATION

We may electronically record and store personal information which we collect from you. When we do so, we will take all reasonable steps to keep it secure and prevent unauthorised disclosure.

However, we cannot promise that your personal information will not be accessed by an unauthorised person (e.g. a hacker) or that unauthorised disclosures will not occur. If we provide you with any passwords or other security devices, it is important that you keep these confidential and do not allow them to be used by any other person. You should notify us immediately if the security of your password or security device is breached, this will help prevent the unauthorised disclosure of your personal information.

Some information we hold about you will be stored in paper files, but most of your information will be stored or processed electronically using third-party digital and cloud service providers - see "Third-party digital and cloud service providers" below.

We use a range of physical and electronic security measures to protect the security of the personal information we hold, including:

- Access to information systems is controlled through identity and access management;
- Our buildings are secured with a combination of locks, monitored alarms and cameras to prevent unauthorised access;
- Employees are bound by internal information security policies and are required to keep information secure;
- Employees are required to complete training about information security and privacy;
- When we send information overseas or use service providers to process or store information, we put arrangements in place to protect your information;
- We regularly monitor and review our compliance (and our service providers' compliance) with internal policies and industry best practice.
- We only keep information for as long as we need it, or as long as the law requires us to. We have a records management policy that governs how we manage our information and records to make sure we destroy any information that is outdated, irrelevant or unnecessary.

5.1 THIRD-PARTY DIGITAL AND CLOUD SERVICE PROVIDERS

We use third-party cloud, software, website, social-media, messaging and artificial-intelligence providers to communicate with clients, manage our practice, process accounting information, administer entities, support professional workflows, host digital platforms and store records. The material providers we currently use are listed below. Locations are based

on provider information available as at October 2026. Where a single country cannot reasonably be identified because a provider uses distributed infrastructure, multiple data centres, affiliates or subprocessors, we state that the exact location cannot be identified and explain why.

Google Workspace (Google): Gmail, Calendar, Drive, Docs, Sheets, Meet and related services are used for email, collaboration and document storage/processing. Google uses distributed global infrastructure. For data not covered by a configured Data Region, Google may store or process data wherever Google or its subprocessors maintain facilities. Eligible Workspace editions can apply supported data-region controls, including the United States or Europe, to specified data. A single country cannot therefore be identified for all Workspace data.

Xero (NZ) Limited / Xero group: Xero Accounting, Xero Practice Manager and related services are used for accounting records, workflow, tax and practice management. Xero states that personal data may be transferred to and processed in Australia, New Zealand and the United States because of its teams and data-hosting locations, and that data may be replicated between data centres in different locations. A single fixed data-centre location cannot be identified for all client data.

Dropbox: Dropbox is used for cloud file storage and document sharing. Our current stated Dropbox storage location is the United States. Dropbox also offers alternative storage regions for eligible team plans, including Australia, the European Union, Japan and the United Kingdom. If our configured region changes, we will update our disclosure where required.

Wolters Kluwer - CCH Entities and related CCH products: We use CCH Entities, including company and trust administration functions, and may use related Wolters Kluwer / CCH products for practice management, compliance, document management, electronic signing, research, workflow or other professional purposes. CCH Entities is a cloud-based service and may contain entity information, director, shareholder, trustee, beneficiary, associated-person, contact, AML/CDD and supporting document information. Wolters Kluwer uses cloud infrastructure for its online products. Public information for CCH Entities does not identify one fixed storage country for every item of CCH Entities data, and storage or processing locations may depend on the product, service, configuration, infrastructure and subprocessors used from time to time.

OpenAI - ChatGPT and related artificial-intelligence services: We may use ChatGPT and related OpenAI services as professional-support tools for drafting, summarisation, research assistance, document review, workflow support and administrative tasks. Where appropriate, information supplied to ChatGPT may include information relevant to a client engagement. We do not intentionally provide client information where it is unnecessary for the task. OpenAI states that, for its business offerings, customer inputs and outputs are not used to train or improve its models by default. OpenAI uses global cloud infrastructure and subprocessors. Eligible business customers may be able to select data residency for certain customer content in supported regions, including Australia, but data residency does not necessarily mean that all processing, safety

monitoring, metadata or integrated services occur only in that region. Accordingly, a single storage or processing country cannot be identified for every item of information processed through ChatGPT unless our applicable workspace configuration and service terms provide otherwise.

Wix.com Ltd. and affiliates (Wix): Wix is used to host and operate our website and may support website forms, online chat, bots, analytics and related digital functions. Wix states that site-visitor personal information may be stored in data centres in the United States, Ireland, South Korea, Taiwan and Israel, and may also be processed in other countries by Wix group companies and third-party processors as necessary to provide its services. Because the particular location can vary by Wix service and routing, Canterbury Accountants cannot identify one single storage country for every item of Wix data.

Meta group services (Facebook, Messenger and Instagram) and WhatsApp: We may use these services for social-media presence, enquiries, messaging and client communications. Meta and WhatsApp operate using global infrastructure, affiliates, data centres and service providers, including infrastructure in the United States and other countries. Canterbury Accountants cannot identify the exact storage or processing location for a particular message or item of content because routing, replication and storage are controlled by the provider and may vary by service, account and user location.

WeChat / Tencent group: We may use WeChat for messaging and client communications. WeChat is operated within the Tencent group and uses provider-controlled infrastructure that may vary according to the relevant service and user location. Canterbury Accountants cannot identify a single storage or processing country for all WeChat information because routing, storage and any use of affiliates or subprocessors are controlled by the provider. We recommend that sensitive accounting, tax, banking or identity information is not sent through WeChat unless we specifically request it and consider that channel appropriate.

Other providers: We may use additional third-party providers from time to time, for example electronic-signature, video-meeting, cyber-security, backup, analytics, marketing, payment, courier, identity-verification, AML/CFT, tax, accounting, artificial-intelligence or specialist software providers. Where a new provider will receive confidential information in connection with our professional services, we will identify the provider and service and disclose the storage or processing location where identifiable, or explain why a single location cannot be identified, before disclosure where required.

Your authorisation: By accepting our engagement, you authorise us to use the providers listed in this Privacy Policy and to disclose confidential and personal information to them to the extent reasonably required for the relevant service. We remain responsible for our privacy obligations where a service provider acts as our agent for storage or processing. We may update the provider list from time to time; where a change materially affects the use or disclosure of client confidential information, we will communicate the relevant provider details and obtain any additional permission required before the disclosure.

5.2 TIMEFRAMES FOR KEEPING PERSONAL INFORMATION

We retain personal information only for as long as it is needed for lawful business, professional, regulatory or legal purposes. When information is no longer required, we take reasonable steps to securely destroy or permanently de-identify it.

Different records may have different retention periods. For many accounting and tax records, records must be retained for at least seven years. Other records may be retained for longer or shorter periods where required or permitted by law, professional standards, regulatory requirements, insurance requirements or our records management policy.

We have a records management policy that governs how we manage our information and records to enable us to destroy any information that is outdated, irrelevant or no longer necessary.

5.3 IF THERE IS A PRIVACY BREACH

We work hard to keep your personal information safe. However, despite applying strict security measures and following industry standards to protect your personal information, there is still a possibility that our security could be breached. If we experience a privacy breach, where there is a loss or unauthorised access or disclosure of your personal information that is likely to cause you serious harm, we will, as soon as we become aware of the breach:

- Seek to quickly identify and secure the breach to prevent any further breaches and reduce the harm caused;
- Assess the nature and severity of the breach, including the type of personal information involved and the risk of harm to affected individuals;
- Advise and involve the appropriate authorities where criminal activity is suspected;
- Where appropriate, notify any individuals who are affected by the breach (where possible, directly);
- Where appropriate, put a notice on our website advising our clients of the breach; and
- Notify the Privacy Commissioner.

6 DISCLOSURE OF YOUR PERSONAL INFORMATION

We may disclose your personal information to others outside Canterbury Accountants where:

- It is necessary to enable us to achieve the purpose that we collected the information for;
- We are required or authorised by law or where we have a public duty to do so;
- You have expressly consented to the disclosure or your consent can be reasonably inferred from the circumstances; or

- We are permitted to disclose the information under the Privacy Act 2020.

6.1 PARTIES WE MAY DISCLOSE YOUR INFORMATION TO

Your personal information may be used by us for the purpose of providing advice and services to you and may also be used by agencies such as, but not limited to:

- Any out-sourced service provider who assists in the services we are required to carry out such as auditors and external compliance reviewers;
- Our external dispute resolution service;
- The Regulator;
- Credit reporting and debt collecting organisations;

If we do not need to share your information with a third party in order to provide advice or services to you, we will not do so unless another lawful basis applies. We do not sell your personal information. Any commissions or other benefits disclosed in our Terms of Business relate to software or insurance products or services, not to the sale or disclosure of your personal information.

6.2 SENDING YOUR INFORMATION OVERSEAS

Some of our service providers store or process information outside New Zealand. Where a provider acts only as our agent for storage or processing, we remain responsible for that information under the Privacy Act 2020 as applicable. Where information is disclosed overseas for the recipient's own purposes, we will comply with the applicable requirements for overseas disclosure, including Information Privacy Principle 12 where applicable, ensuring appropriate safeguards or obtaining informed authorisation where required.

Using an overseas service provider does not reduce our commitment to protect your information. We use contractual, technical and organisational safeguards appropriate to the nature of the information and the services involved.

Privacy and information-protection laws differ between countries. We assess the privacy and security arrangements of material service providers and review them periodically. If a proposed disclosure requires your specific informed authorisation under the Privacy Act 2020, we will obtain that authorisation before making the disclosure.

6.3 THIRD PARTY WEBSITES

Through our website or our other social media pages, you may be able to link to other websites which are not under our control. We are not responsible for the privacy or security practices of those third-party websites and the sites are not covered by this Privacy Policy. Third party websites should have their own privacy and security policies and we encourage you to read them.

In addition, we have no knowledge of (or control over) the nature, content, and availability of those websites. We do not

sponsor, recommend, or endorse anything contained on these linked websites. We do not accept any liability of any description for any loss suffered by you by relying on anything contained or not contained on these linked websites.

7 RIGHT TO ACCESS AND CORRECT PERSONAL INFORMATION; REQUESTS FOR DELETION

You have the right under the Privacy Act 2020 to request access to personal information we hold about you and to request correction of that information. You may also ask us to delete personal information, but the Privacy Act 2020 does not create a general right to deletion and we may need to retain information to comply with legal, regulatory, professional, insurance, contractual or legitimate business requirements. You can make a request by contacting us at:

PO Box 7115
Sydenham
Christchurch 8240
Or via email at admin@canterburyaccountants.co.nz

When you contact us with a request, we will address it within a reasonable period. For access and correction requests, we will respond in accordance with the Privacy Act 2020. We will also consider deletion requests, subject to any legal, regulatory, professional, insurance, contractual or legitimate business requirement to retain the information. To protect the security of your personal information, we may require identification before providing access or making changes.

We may delete personal information where appropriate, but we may retain it where required or permitted by law, professional standards, regulatory requirements or our records management obligations.

There is generally no fee for requesting access to or correction of your personal information. We do not charge for considering a deletion request. A reasonable charge may apply to an access request only where permitted by the Privacy Act 2020.

There are circumstances in which we may refuse access to or correction of personal information under the Privacy Act 2020. If we refuse an access or correction request, we will explain our reasons unless the law prevents us from doing so. If we decline a deletion request, we will explain the reason where practicable.

If we refuse to correct your personal information, you may request that a statement of correction be attached to the information noting the correction you requested.

If we refuse a request for access to or correction of your personal information, we will also provide information about how you can complain about the refusal.

8 WHAT HAPPENS IF YOU DO NOT PROVIDE US YOUR INFORMATION?

If you do not provide information we have requested, you may be unable to obtain or access our services for which the information is required. Please ask us if you are unsure what information is important and how this might affect you.

9 CHANGES TO THIS PRIVACY POLICY

We review this Privacy Policy periodically to keep it current and available on our website. If changes materially affect how we use or disclose client confidential or personal information, we will communicate the relevant changes and obtain any additional permission required before the disclosure where required. You may also obtain a copy of the latest version by calling us on 03 366 5776.

10 PRIVACY POLICY QUERIES AND CONCERNS

If you are concerned about how your personal information is being handled or if you feel that we have compromised your privacy in some way, please contact us at:

Level 1
Unit 2/15 Washington Way
Sydenham
Christchurch 8011

03-366 5776

admin@canterburyaccountants.co.nz

We will acknowledge your complaint within three working days of its receipt. We will let you know if we need any further information from you to investigate your complaint.

We aim to resolve complaints as quickly as possible. We strive to resolve complaints within five working days, but some complaints take longer to resolve. If your complaint is taking longer, we will let you know what is happening and a date by which you can reasonably expect a response.

If you are not satisfied with our response to a privacy-related concern, you may complain to the Office of the Privacy Commissioner at www.privacy.org.nz or by using the contact details published by that Office.

Office of the Privacy Commissioner

P O Box 10-094
Wellington 6143, New Zealand

Email: enquiries@privacy.org.nz

Telephone: 0800 803 909

Website: www.privacy.org.nz

[This page is intentionally left blank.]