

Privacy Policy

Effective date: 17 April 2026

1 This Privacy Policy

1.1. About this Privacy Policy

Caleb and Brown Pty Ltd (ABN 66 619 023 559) and its related bodies corporate (collectively, **Caleb & Brown, we, us and our**) understand that your privacy is paramount, and are committed to protecting your privacy.

This privacy policy (**Privacy Policy**) describes the handling of personal information by us, including through our website (www.calebandbrown.com) (**Website**), the Caleb & Brown self-directed trading portal and the Caleb & Brown mobile application (**C&B App**).

Unless you notify us otherwise, by accessing our services or providing your personal information, you consent to the collection, use and disclosure of your personal information as described in this Privacy Policy.

We may modify or revise this Privacy Policy from time to time, including whenever there are changes to regulations or our business operations. Any changes published on the Website will be taken to be effective when they are published and the changes supersede all prior versions. We recommend you check our Website regularly to ensure you are aware of the current Privacy Policy.

1.2. Personal information controller

A personal information controller is a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on their behalf.

Caleb & Brown is the personal information controller for the information it collects from you in accordance with this Privacy Policy:

Caleb & Brown
Level 4, 33 Cremorne St
Cremorne VIC 3121, Australia

2 What personal information do we collect?

2.1. Personal information

When we refer to personal information, we mean information or an opinion about an individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in material form or not.

The kinds of personal information that we collect and hold about you depends on your dealings with us. Examples of personal information we collect and hold include:

- name;

- date of birth;
- residential address;
- email address;
- nationality;
- cryptocurrency wallet ID, address and transactions;
- mobile phone number;
- copies of, or details from, identification documents;
- the purpose of your cryptocurrency transactions and source of funds;
- financial information (such as your bank account details and statements and credit card details);
- if relevant, politically exposed persons match results; and
- qualifications and employment history, in the event you are applying for a job or contract with us.

We may also collect other personal information we consider is reasonably necessary for one or more of our functions and activities such as personal information that we request from you or that you or a third party provide to us, and which we are authorised or required by law to collect.

2.2. Sensitive information

We may also collect sensitive information about you if you consent to us doing so and the information is reasonably necessary for one or more of our functions or activities, or where otherwise permitted or required by law.

The kinds of sensitive information that we collect and hold about you depends on your dealings with us. Examples of sensitive information we collect and hold include biometric data, or information on your racial or ethnic origin which may be included in your identification documents.

Where we collect sensitive information, we will only process it:

- to verify your identity;
- to perform a contract with you or to carry out our business in relation to that contract;
- where we have legitimate interests to process the personal data and they're not overridden by your rights;
- in accordance with a legal obligation; or
- where we have your consent.

We will retain your information only for as long as is necessary for the purposes set forth in this Privacy Policy, for as long as your account remains active, or as needed to provide you with any services you request from us. We will retain and use your information to the extent necessary to comply with our legal obligations.

3 How we collect your personal information

We will usually collect your personal information directly from you, such as by telephone, video call, standard form, letter, email, or via you visiting our Website or C&B App.

We may also collect your personal information from a related entity or from a third party or a publicly available source where it is unreasonable or impractical to collect the personal information directly from you or if necessary to satisfy our legal obligations. For example, we may collect know-your-customer (**KYC**) or anti-money laundering and countering the financing of terrorism (**AML/CFT**) information about you from our identity-verification services provider(s). We also often collect your name, address, proof of address and date of birth from our identity-verification services provider(s).

We may also collect your personal information (such as your name, address, date of birth, biometric information) during telephone or video calls by recording or transcribing the call.

If you are a company director or shareholder of a trust or company that uses our Website or C&B App, then we may collect your personal information (such as name, address and date of birth) from the relevant corporate regulator.

If you apply for a position or contract as an employee or service provider with us, we may also collect personal information about you from your nominated referees.

There may be occasions when we receive unsolicited personal information about you. In such instances, unless it is reasonably necessary for one or more of our functions or activities, or we are otherwise permitted or required by law to retain it, we will de-identify or destroy it as soon as reasonably practicable provided it is lawful and reasonable to do so.

If we don't collect your personal information, we may be unable to provide you with all of our services, and some functions and features on our Website and C&B App may not be available to you.

4 Collection of information through our Website

Our web servers may automatically collect information when you visit our Website, including:

- your internet protocol (**IP**) address;
- the date and time of your visit;
- the parts of our Website you access during your visit;
- your actions on our Website; and
- the operating system and browser you are using.

In using our Website, your personal information may be collected through the use of cookies. These are small text files placed on your mobile device or computer by our Website which automatically collect information about you without you providing that information to us directly. Cookies are not malicious programs that access or damage your computer, tablet or smartphone.

We use cookies to understand and save your preferences for future visits and compile aggregate data about site traffic and site interaction so that we can offer better site experiences and tools in the future.

Most devices automatically accept cookies but you can choose to reject cookies by changing your device settings. However, please note that rejecting cookies may mean that some or all of the functions on our Website will not be available to you.

Sometimes our Website contains links to other websites. When you access a website other than our Website, we are not responsible for the privacy practices of that website. We recommend that you review the privacy policies of each website you visit.

5 Collection of information through the C&B App

In using the C&B App, we may collect and receive information about you from the iOS or Android app stores and other vendors, such as the IP address of your mobile device, the mobile operating system, the type of mobile internet browsers you use, and information about the way you use the C&B App. The C&B App may send information to us that you authorize.

When you use the C&B App, we may collect certain information directly from your device such as a unique mobile device identification number, the IP address of your mobile device, the mobile operating system, the type of mobile internet browsers you use, and information about the way you use the C&B App. This information is used in an aggregated manner to analyze how people use the C&B App, such that we can improve our service. We may also use global positioning system (or similar) technology to determine your current location in order to determine the city in which you are located and display a location map with relevant advertisements. We will not share your current location with other users or partners.

We may from time to time use cookies on the C&B App. These are small text files which a mobile application uses to collect information about you without you providing that information to us directly. Cookies are not malicious programs that access or damage your computer, tablet or smartphone.

Most devices automatically accept cookies but you can choose to reject cookies by changing your device settings. However, please note that rejecting cookies may mean that some or all of the functions on our mobile application will not be available to you.

Sometimes the C&B App contains links to other applications or websites not controlled by us. When you access such other application or website, we are not responsible for the privacy practices of that application or website. We recommend that you review the privacy policies of each application or website you visit.

6 How we use your personal information

In order to provide our services to you, we are required to collect and process your personal information (including sensitive information) for our KYC obligations under various applicable laws and regulations (including AML/CFT laws).

Personal information we collect may also be used for the following purposes:

- **To communicate with you.** This may include:
 - to facilitate and process your orders and transactions (for example, by using your personal information to send transactional communications via email to confirm your trades);
 - providing you with information you've requested from us or information we are required to send to you;

- administrative communications, like changes to the Website and services, security updates, or assistance with using our Website and services;
 - to send notifications to you (via email, SMS/text message or by other means) related to your orders, transactions as well as legal and security alerts; and
 - asking you for feedback or to take part in any research or survey we are conducting (which we may engage a third party to assist with);
- **To market to you.** This may include marketing communications about our cryptocurrency brokerage (www.calebandbrown.com), our cryptocurrency managed funds (funds.calebandbrown.com) or another product, service, or information we think you might be interested in) via any medium including email, telephone or other media (though we will always allow you to unsubscribe from such marketing or promotional communications);
 - **To provide updates on the market.** This may include sending you news, newsletters, broker reports, articles and other similar material that we think may be of interest to you;
 - **To protect you.** So that we can detect and prevent any fraudulent or malicious activity (including security incidents), and make sure that everyone is using our Website and services fairly and in accordance with our terms and conditions;
 - **To support you.** This may include assisting with the resolution of technical support issues or other issues relating to the Website or services, whether by email, in-app support or otherwise;
 - **To hire you.** We may use your personal information to assess your application for a position or contract as an employee or service provider with us;
 - **To enhance our Website and services and develop new ones:** For example, by tracking and monitoring your use of our Website and services so we can keep improving, or by carrying out technical analysis of our Website and services so that we can optimize your user experience and provide you with more efficient tools;
 - **To resolve disputes.** We may use transcripts or call recordings (which contain personal information) between you and us in order to investigate and help resolve any disputes or complaints you may have;
 - **To analyze, aggregate and report.** We may use your personal information (whether obtained directly or from third parties) to produce aggregated and anonymised analytics and reports, which we may share publicly or with third parties;
 - **To make decisions in relation to your use of our website and services.** We may use your IP address to determine which country you are from and, based on such IP address, make a decision about whether or not to allow you access to our website and/or our services. We may also use automated decision-making processes to identify scam or fake data amongst emails; and
 - **To comply with legal obligations.** Where we believe it is necessary to comply with our legal obligations, including under AML/CFT laws, or to investigate, prevent or take action regarding suspected illegal activities, potential threats to the safety of any person, or violations of our

website terms and conditions or this Privacy Policy. As the law often requires us to inform you of certain changes to our products/services and regulatory changes, we may, from time to time, use your personal information to send out email notifications to keep you informed.

7 How we hold your personal information

We typically hold your personal information in information technology (**IT**) systems, including IT systems operated for us by our service providers. We take reasonable steps to safeguard personal information and ensure its protection from misuse, interference, loss, unauthorised access, modification or disclosure, including having appropriate security measures in place to protect electronic materials. Additionally, we require our service providers to also have appropriate security measures in place.

We secure electronic records within our network databases, and through third party data storage providers. This includes, but is not limited to, ensuring that personal information within our network is password protected, with access appropriately limited and monitored. Our service providers, including third party data storage providers, are required to protect personal information in accordance with applicable laws and take appropriate technical and organization measures against unauthorised or unlawful use of personal information or its accidental loss, destruction or damage.

8 How we share your personal information

8.1. Disclosure to third parties

At times, we may provide your personal information to trusted third parties, in order to provide all the functionalities that we offer through our Website or C&B App. We do not provide customer personal information to third-parties for marketing; however, some clients may receive marketing materials from us relating to assets that they currently own, previously owned or are interested in. We do not sell your personal information or sensitive information.

Third parties with whom we may share your personal information include:

- our related entities;
- third party service providers who help facilitate business operations, such as identity-verification, payment processing, IT and email marketing services providers;
- financial institutions for payment services;
- parties to whom you have requested we disclose personal information;
- prospective service providers and business partners; and
- government, regulatory or law enforcement agencies.

Where information is shared with these third parties, we will take all reasonable steps to ensure that third parties observe the confidential nature of such information and are prohibited from using any or all of this information beyond what is necessary to assist us.

For clarity, we do not sell or share your personal information (including mobile information) with these third parties for their own marketing or promotional purposes.

8.2. Overseas disclosure

When we share personal information, it may be transferred to, and processed in, countries other than the country you live in. Some of our service providers and related companies are located both inside and outside of Australia. Additionally, certain cloud storage and IT servers may be located both inside and outside of Australia.

Rest assured, where we disclose personal information to a third party in another country, we put safeguards in place requiring the third party to ensure your personal information remains protected. These safeguards usually include contractual obligations placed on the recipient to ensure that they comply with all applicable laws in relation to their handling of such personal information. Please contact us if you would like further details regarding these obligations.

8.3. Disclosure to law enforcement or government agencies

We may disclose your personal information to law enforcement or government agencies where we are required to do so by law or under court order. Where permitted by law, we will endeavor to give prior notice to our customers whose data is requested by any government or law enforcement agency. If we are unable to provide prior notice, then we will endeavor to give notice as soon as reasonably practicable.

We may not notify you if it is prohibited by law and in certain exceptional circumstances at our sole discretion, such as emergencies, when notice could result in danger or personal harm, or when notice would be counterproductive (for example, when the user's email has been compromised).

8.4. Disclosure of de-identified information

We may share aggregated or de-identified information with third parties for research, marketing, analytics and other purposes, provided that this information does not identify particular individuals.

8.5. Identify verification and government-related identifiers

We have obligations under various AML/CTF laws across the globe, including Australia and the United States of America. This includes legal obligations to verify and confirm your identity (sometimes known as KYC or CDD) before we can provide any regulated services, and at certain other times in the course of us providing services to you. These procedures are fundamental to our commitment to identify, mitigate and manage the risks of money laundering and terrorism financing. Any government-related identifiers obtained for the purposes of identification will be used or disclosed only for the following purposes:

- as required or authorised by or under any applicable law or a court/tribunal order;
- where reasonably necessary for us to fulfil our legal obligations; or
- where reasonably necessary for us to verify the identity of the individual for the purposes of our compliance obligations, functions or activities.

To meet our Australian legal obligations, we may use the Australian Government's Document Verification Service (**DVS**) to verify the identity of Australian customers. The DVS allows for the validation of government-issued identity documents (eg, passports, driver's licences) by comparing provided details against the records held by the respective Australian government issuing authority. The DVS checks the details you provide against the records of the document's issuing agency and provides a 'match' or 'no

match' response. You have the right to know how your information is collected and used for this purpose. If you decline to have your identity verified through this process, we may be unable to provide you with our services. For information about making a complaint regarding our handling of your information for this purpose, please see section 10 of this policy. You can find further details on the DVS from the Department of Home Affairs by visiting their website at the following link: <https://www.idmatch.gov.au/resources/identity-verification-services-privacy-statement>.

9 Accessing and correcting your personal information

Depending on the country in which you reside, you may have certain rights with respect to your personal information:

- **Withdraw consent or object to process.** In certain circumstances, applicable law may allow you to object to our processing of your personal information. Further, if you provided your consent to our processing of your personal information, you may withdraw such consent, though doing so will not affect the lawfulness of our processing based on consent before your withdrawal;
- **Know and access what personal data we hold about you.** Subject to the exceptions set out under applicable law, you may obtain confirmation from us as to whether or not we process your personal information, and, if so, obtain access to the personal information we hold about you. You may be required to put your request in writing for security reasons. We may in certain circumstances charge you a reasonable fee to meet our costs in providing you with details of the personal information we hold about you if your request requires a material effort on our part. We will communicate any costs to you before completing your request. If we refuse to provide you with access to the information, we will provide you with reasons for the refusal and inform you of any exceptions relied upon under applicable law (unless it would be unreasonable to do so);
- **Correct or update your personal information.** We take reasonable steps to ensure that your personal information is accurate, complete, and up-to-date whenever we collect or use it. If you believe that the personal information we hold about you is out of date, incomplete or incorrect, you may request that the personal information be updated or amended. We will take reasonable steps to either correct this information, or if necessary, discuss alternative action with you; and
- **Ask us to restrict processing your personal data or delete it.** In accordance with applicable law, you may also be entitled to request that your personal information be erased.

Depending on your jurisdiction, you can exercise these rights at any time by sending an email to support@calebandbrown.com with the subject like "Data Subject Request." We do not discriminate in any way against you for exercising your personal information rights. We may request some information from you such as your name, email address, and account information when you submit a request in order to verify your identity.

10 Complaints

If you believe that we have not dealt with your personal information in a manner that complies with privacy laws or this Privacy Policy, please let us know by sending an email to support@calebandbrown.com so that we can properly address and resolve your concerns. We take any privacy complaint seriously. If you

make a complaint, we will review and investigate your complaint and get back to you in a timely and efficient manner.

If you are an Australian resident and are dissatisfied with our response, you have the right to make a complaint to the Office of the Australian Information Commissioner by phoning 1300 363 992 or by email at enquiries@oaic.gov.au.

11 Opt out of communications

If you prefer not to receive promotional communications from us, you may opt out by using the unsubscribe link within each email or by contacting your broker directly or by contacting us as provided below to have your contact information removed from our promotional mail list.

Please note that after opting out of promotional communications, you will continue to receive transactional communications and important legal and security alerts and notifications from us.

12 Our contact details

For more information about this Privacy Policy please address your enquiry to the Data Protection Officer, Level 4, 33 Cremorne St, Cremorne, VIC 3121 or contact us by email at support@calebandbrown.com.

13 Jurisdiction specific terms

13.1. Children's Personal Information and Online Privacy

The Children's Online Privacy Protection Act (**COPPA**) is intended to provide parents in the United States of America increased control over what information is collected from their children online and how such information is used. The law applies to websites and services directed to, and which knowingly collect information from, children under the age of 13.

Our products and services are not directed to persons under the age of 18 (**Children or Child**) and we do not knowingly collect personal information from Children. If we learn that we have inadvertently gathered personal information from a Child, we will take legally permissible measures to remove that information from our records. We will require the user to close their account and will not allow the continued use of our products and services.

If you are a parent or guardian of a Child, and you become aware that a Child has provided personal information to us, please contact us as support@calebandbrown.com. If you are a Child, please do not provide any personal information to us. For additional information on COPPA protections, refer to the Federal Trade Commission's website.

13.2. Gramm–Leach–Bliley Act

Under the Gramm–Leach–Bliley Act (**GLBA**), financial institutions are required to disclose their information–sharing practices and give customers the ability to opt out of certain personal information disclosures. Details are outlined in this Privacy Policy, but if you have any additional questions, please contact us at support@calebandbrown.com.

Other important information:

State	Notes
Vermont	If you are a customer residing in Vermont, we will not share information we collect about you with companies outside of Caleb and Brown Limited, unless the law allows. We will not disclose information about your creditworthiness to our affiliates and will not disclose your personal information, financial information, credit report, or health information to non–affiliated third parties to market to you, other than as permitted by Vermont law, unless you authorize us to make those disclosures.