SNOWBALL X PRIVACY POLICY

Updated and effective: 28 July 2026

1. About this Policy

SNB Finance Holdings Limited (NZBN 9429046386212), trading as Snowball X and Snowball Securities (SNB, we, us or our), is the New Zealand agency that collects and holds the personal information described in this Policy. Our registered office is Tenancy 1, Level 11, Tower II, 205 Queen Street, Auckland 1010, New Zealand.

This Policy explains how we collect, hold, use, disclose, protect and dispose of personal information when you apply for or use our financial services, websites, mobile applications, customer support channels and related products or features (Services). It applies to customers and other individuals whose personal information we handle, whether they are located in New Zealand or overseas.

We comply with the Privacy Act 2020, including the information privacy principles (IPPs) and IPP 3A on indirect collection, and with any applicable code of practice. Biometric processing is also governed by the Biometric Processing Privacy Code 2025 (Biometric Code). Our identity-verification practices take account of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) and, where applicable, the Identity Verification Code of Practice 2026 (IVCOP 2026).

This Policy is a customer-facing privacy statement. It may be supplemented by a shorter notice at the point we collect particular information, including a biometric notice. A more specific notice applies to the extent that it gives you additional information about a particular collection. Nothing in this Policy limits rights or protections that cannot lawfully be limited.

Key points

- We collect only personal information that is reasonably necessary for lawful purposes connected with our Services.
- Some information is required by law or is necessary for us to open, operate or protect your account. If you do not provide it, we may be unable to provide or continue the relevant Service.
- We may collect personal information indirectly from public registers, sanctions and politically exposed person screening sources, brokers, custodians, banks and other third parties. We may also collect or generate identity-verification information through electronic identity-verification providers acting on our behalf. Where IPP 3A applies, we will take reasonable steps to notify you of the indirect collection and the matters required by IPP 3A, unless an exception under the Privacy Act applies.
- Some service providers, personnel, brokers or custodians may be overseas, including in Hong Kong SAR and the United States. We remain responsible for agents that process information solely on our behalf and apply the safeguards required for overseas disclosures.
- You may request access to or correction of your personal information and may complain to our Privacy Officer or the Office of the Privacy Commissioner.

Your use of the Services does not, by itself, waive any privacy right or amount to an express authorisation where the Privacy Act or the Biometric Code requires us to obtain one.

2. Personal Information We Collect

Personal information means information about an identifiable individual. It may include information that identifies you directly and information that can identify you when combined with other information. Some information we handle—such as identity documents, financial information and biometric information—is particularly sensitive and receives safeguards appropriate to its sensitivity.

Depending on your relationship with us and the Services you use, we may collect the following categories:

- **Identity and contact information:** full name, aliases, date and place of birth, nationality, citizenship, residential and mailing addresses, email address, telephone number, signature, username and customer or account identifiers.
- **Tax and regulatory information:** tax residence, tax identification numbers, declarations required under FATCA or the Common Reporting Standard, and information required to assess legal or regulatory eligibility.
- **Customer due diligence information:** passports and other identity documents, photographs, verification records, beneficial ownership and control information, authority to act, source of funds, source of wealth, sanctions and politically exposed person screening results, and other information required for standard, simplified, enhanced or ongoing customer due diligence.
- **Biometric information used for remote identity verification:** live facial images or video, liveness-detection information, and any biometric template, comparison result or verification outcome generated by the identity-verification process. Section 5 explains this processing.
- **Financial and account information:** occupation and employment details; income, assets, net worth and financial position; bank and payment details; account balances; deposits, withdrawals and transfers; and information relevant to account funding or withdrawals.
- **Investment and transaction information:** investment experience and objectives, risk and product preferences, holdings, orders, trades, execution details, corporate actions, market subscriptions and transaction history.
- **Technical and usage information:** device type and operating system, device and application identifiers where necessary, IP address, network and security logs, authentication events, language and notification settings, cookie or similar technology data, and information about how you interact with our Services.
- **Communications and support information:** messages, enquiries, complaints, survey responses and records of online or telephone support. Calls or other communications may be recorded where we tell you or where recording is otherwise lawful.
- **Preferences and records we create:** communication and marketing preferences, internal account notes, fraud and security alerts, compliance assessments, risk ratings and records of decisions made in administering the relationship.

We do not seek information that is excessive or unrelated to the purposes described in this Policy. We periodically review forms, permissions and data fields to support data minimisation.

3. How We Collect Personal Information

3.1 Direct collection

We usually collect personal information directly from you—for example, when you register, apply for an account, complete customer due diligence, fund or operate an account, place an order, change settings, contact us or use our website or applications. We may also generate technical, transaction and security records when you use the Services.

At or before collection, we take reasonable steps to make you aware of SNB's identity and address, why the information is being collected, the intended recipients, whether collection is authorised or required by law, whether providing it is mandatory or voluntary, the consequences of not providing it, and your rights of access and correction. This Policy and any point-of-collection notice work together to provide that information.

3.2 Indirect collection

Where permitted by IPP 2 or another law, we may collect personal information about you from:

- identity and address verification providers, and providers that check the authenticity of documents or perform facial and liveness verification;
- public registers, company records, professional databases, media, and sanctions, law-enforcement or politically exposed person sources;
- execution brokers, custodians, banks, payment providers, exchanges and other financial institutions involved in providing or supporting the Services;
- our related companies, contractors and service providers;
- your authorised representative, employer, trustee, director, shareholder, beneficial owner or other person connected with an account; and
- regulators, government agencies, courts, dispute-resolution bodies or law-enforcement agencies, where lawful.

When we collect personal information from someone other than you, we take reasonable steps to notify you as soon as reasonably practicable of the matters required by IPP 3A, including the fact of collection and the circumstances in which it occurred, unless you have already been made aware or a statutory exception applies. Where notification could prejudice fraud detection, an investigation, the maintenance of the law or another protected interest, we assess and record the applicable exception rather than treating it as automatic.

4. Why We Collect and Use Personal Information

We collect and use personal information only for lawful purposes connected with our functions and activities, including to:

- assess applications; establish, administer, monitor, suspend or close accounts; and manage our relationship with you;
- identify and verify you and connected persons; conduct customer due diligence and ongoing monitoring; screen for sanctions and politically exposed persons; and comply with the AML/CFT Act, IVCOP 2026 and related legal or regulatory obligations;
- receive and carry out account, funding, withdrawal, transfer, order and trading instructions; arrange execution, clearing, settlement and custody; and provide statements, confirmations and other account records;
- verify authority to act and protect your account, our systems and other customers against identity theft, fraud, cyber threats, misuse and other unlawful activity;

- comply with financial-services, tax, record-keeping, reporting, court, regulatory, law-enforcement and dispute-resolution obligations in New Zealand or another applicable jurisdiction;
- communicate with you about the Services, material terms, security, transactions, service interruptions, complaints and changes to this Policy;
- provide market information, alerts, questionnaires and promotional communications where permitted and in accordance with your preferences. You may unsubscribe from marketing without losing essential service communications;
- operate, test, audit, secure, analyse and improve our Services, systems, controls and customer support; and
- establish, exercise or defend legal rights and manage audits, insurance, complaints, incidents, business continuity or corporate transactions.

We do not use personal information for a materially different purpose unless that use is authorised by you or otherwise permitted by the Privacy Act. Before using information, we take reasonable steps to ensure it is accurate, up to date, complete, relevant and not misleading for the proposed use.

5. Biometric Information and Liveness Verification

5.1 Account-opening identity verification

For remote identity verification, SNB or an appointed electronic identity-verification provider acting on our behalf may collect a live facial image or video and liveness information through your device camera. The process may generate a facial template, comparison score and verification result by comparing the live image with the photograph in an identity document. SNB remains responsible under New Zealand privacy law for biometric processing carried out by a provider solely as our agent.

We use this biometric information to verify that you are the person shown in the identity document, reduce impersonation and identity fraud, and meet customer-identification and verification obligations under the AML/CFT Act. IVCOP 2026 provides an accepted identity-verification practice where its requirements are followed. We do not use account-opening biometric information for marketing, emotion recognition, or to infer ethnicity, sex, health or other protected characteristics.

Before using biometric processing, we assess whether it is necessary, effective and proportionate for the particular purpose and implement reasonable safeguards. At or before collection, we tell you what biometric information is collected, the specific purpose, intended recipients, whether it is required, the consequences of declining, your access and correction rights, and any alternative verification method that is actually available. If no compliant alternative is available and you do not complete verification, we may be unable to open or continue your account.

Biometric information may be processed or accessed outside New Zealand by the identity-verification provider or its approved subprocessors. Sections 7 and 8 apply to that processing. We retain raw images, templates and liveness information only for as long as reasonably necessary for verification, fraud prevention, audit, complaint handling and any applicable legal record-keeping requirement. A verification record that must be retained under the AML/CFT Act may be kept for the statutory period; biometric material that is not required for those purposes is deleted or de-identified sooner.

5.2 Face ID or fingerprint authentication on your device

If you enable Face ID, fingerprint or another device-level biometric method to authenticate login or trading instructions, the biometric feature is stored and matched by your device and its operating system. SNB does not collect or receive the fingerprint, facial map or biometric template used by the device. We receive only a confirmation that device authentication succeeded or failed, together with related security and authentication logs. You may disable this optional feature and use an available non-biometric authentication method.

Our handling of biometric information is governed by the Biometric Processing Privacy Code 2025, including rule 3A for indirect collection. You may request access to or correction of biometric information held by us and may raise a complaint using the details in section 14.

6. Who We Share Personal Information With

We disclose personal information only where we have a lawful basis under the Privacy Act, the Biometric Code or another applicable law. Depending on the purpose, recipients may include:

- SNB personnel and authorised personnel of related companies who need the information to provide services, customer support, technology, operations, risk or compliance functions;
- identity-verification, screening, cloud, hosting, cybersecurity, communications, analytics, software, records-management and other service providers acting for us;
- execution brokers, custodians, clearing and settlement organisations, exchanges, market-data providers, banks, payment providers and other financial institutions involved in your account or transactions;
- auditors, insurers, lawyers, accountants and other professional advisers subject to confidentiality obligations;
- DIA, the Financial Intelligence Unit, Inland Revenue, the Financial Markets Authority, other regulators, courts, law-enforcement agencies and government bodies where disclosure is required or permitted;
- a prospective purchaser, investor or successor in connection with a proposed merger, restructuring, financing, sale or transfer, subject to appropriate confidentiality and privacy safeguards; and
- another person where you have authorised the disclosure or where an IPP 11 or other statutory exception applies.

We limit disclosures to information reasonably necessary for the relevant purpose. Service providers acting on our behalf must handle personal information only for authorised purposes and must apply confidentiality, security, retention and deletion controls appropriate to the information and the service. We do not sell personal information and do not publicly disclose it except where you have made it public, authorised disclosure, or disclosure is otherwise permitted by law.

7. Service Providers and Agency Processing

A service provider may store or process personal information solely on SNB's behalf. Where section 11 of the Privacy Act applies, that processing is treated as being carried out by SNB rather than as a disclosure to the provider. SNB remains responsible for the provider's handling of the information for the outsourced service.

Before appointing a provider that will handle sensitive or material personal information, we assess relevant privacy and security risks, define the provider's permitted purposes and access, require appropriate safeguards, manage subprocessors and data locations, and address return or secure deletion when the service ends. We monitor the arrangement in a manner proportionate to risk.

8. Overseas Processing and Disclosure

SNB is based in New Zealand, but some authorised personnel and service providers, and some brokers, custodians or technology providers, are located or operate overseas. Accordingly, personal information may be stored, processed or accessed in countries or regions including Hong Kong SAR and the United States.

Where an overseas recipient acts solely as our agent for storage or processing, section 11 applies and SNB remains responsible. Where we disclose personal information to an overseas recipient for that recipient's own purposes, we comply with IPP 12 or, for biometric information, rule 12 of the Biometric Code. This means we must have reasonable grounds for the disclosure—for example, because the recipient is subject to the New Zealand Privacy Act or comparable safeguards, or because binding contractual safeguards provide a comparable level of protection.

If we propose to rely on your authorisation for an overseas disclosure to a recipient that may not provide comparable safeguards, we will first expressly tell you that the information may not receive the same protection as under New Zealand law and will request specific authorisation. We do not treat general use of the Services or acceptance of this Policy as that authorisation.

An overseas recipient may be subject to lawful access requests by courts, regulators or law-enforcement authorities in its jurisdiction. We assess the legal and contractual protections available and disclose only what is reasonably necessary and permitted.

9. Your Privacy Rights

9.1 Access

You may ask whether we hold personal information about you and request access to it. We will respond as soon as reasonably practicable and no later than 20 working days after receiving your request, unless the Privacy Act permits an extension. We may ask for information needed to verify your identity and clarify the scope of the request.

The Privacy Act permits information to be withheld in limited circumstances. If we refuse access in whole or in part, we will normally explain the relevant ground and tell you about your right to complain, unless the law permits us not to do so. Any charge for access will be reasonable and permitted by law, and we will tell you in advance.

9.2 Correction

You may ask us to correct personal information you believe is inaccurate, incomplete or misleading. If we do not make the requested correction, you may ask us to attach a statement of correction to the information. Where appropriate, we will take reasonable steps to inform recipients of a correction.

9.3 Communication preferences and permissions

You may change optional communication preferences, unsubscribe from marketing and manage device permissions through the relevant application or device settings. Withdrawing an optional permission does not affect processing already carried out lawfully. Some information and permissions are necessary to provide or secure a Service; disabling them may make that Service unavailable.

9.4 Account closure and deletion requests

You may ask to close your account or request deletion of information. Account closure does not require us to delete information that must be retained for AML/CFT, tax, financial-services, fraud-prevention, dispute, legal or audit purposes. When no lawful or necessary purpose remains, we securely delete, destroy or de-identify the information.

9.5 Complaints

If you have a privacy concern, please contact our Privacy Officer using section 14. We will acknowledge and investigate the matter, keep you informed where appropriate, and explain our outcome. If you are not satisfied, you may complain to the Office of the Privacy Commissioner at www.privacy.org.nz. You do not lose any other right or remedy by contacting us first.

10. Retention, Security and Privacy Breaches

10.1 Retention

We retain personal information only for as long as it is required for the purpose for which it was collected or another lawful purpose. Retention periods depend on the type of information, the sensitivity and risk, the account and transaction lifecycle, and legal, regulatory, tax, audit, fraud, complaint and dispute requirements.

The AML/CFT Act generally requires specified identity, verification and transaction records to be retained for at least five years after the relevant transaction or activity is completed or after the business relationship ends, depending on the record. A supervisor or another lawful requirement may require a longer period. We may also preserve information subject to a legal hold, investigation or unresolved complaint. When retention is no longer necessary, we securely delete or destroy the information or de-identify it so that it is no longer personal information.

10.2 Security

We use physical, technical and organisational safeguards that are reasonable in the circumstances and proportionate to the sensitivity of the information. These include access controls and least-privilege permissions, authentication measures, encryption in transit and appropriate protection at rest, logging and monitoring, vulnerability and incident-management processes, backups and business-continuity controls, staff confidentiality and training, and service-provider due diligence and contractual controls.

No method of electronic storage or transmission is completely secure. You should protect passwords and devices, use available security features, log out of shared devices and contact us promptly if you suspect unauthorised access or account misuse. These precautions do not reduce SNB’s obligations under the Privacy Act.

10.3 Privacy breaches

If a privacy breach occurs, we will take steps to contain it, assess the information and people affected, mitigate harm, preserve evidence and prevent recurrence. If the 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. Our notice will provide information reasonably required by the Privacy Act and practical steps you can take to protect yourself.

11. Cookies and Similar Technologies

Our websites and applications may use cookies, software development kits, local storage and similar technologies to authenticate you, maintain sessions, remember preferences, protect security, diagnose faults, understand use of the Services and improve performance. We do not use these technologies to collect information unrelated to a stated lawful purpose.

You can manage browser cookies and many application permissions through your browser, device or application settings. Blocking necessary cookies or permissions may prevent login or make parts of the Services unavailable. Where applicable law requires a separate choice for non-essential technologies, we will provide that choice.

12. Children and Young People

Our brokerage Services are intended for adults and we do not knowingly open accounts for persons under 18. If we learn that we have collected personal information from a child without a lawful basis, we will take reasonable steps to delete it, subject to any legal obligation to retain it. A parent or guardian who believes a child has provided information to us should contact our Privacy Officer.

13. Changes to this Policy

We may update this Policy when our Services, information practices, providers or legal obligations change. We will publish the current version and effective date on our website. If a change is material, we will give additional notice through an appropriate channel, such as the application, website, email or account message. We will obtain authorisation where required for a new use or disclosure; merely updating this Policy does not create an authorisation that the law requires to be specific and informed.

14. Contact Us

SNB has appointed a Privacy Officer. To request access or correction, raise a complaint, ask about an indirect collection or overseas disclosure, or make another privacy enquiry, contact:

Privacy Officer

SNB Finance Holdings Limited

Address： Tenancy 1, Level 11, Tower II, 205 Queen Street, Auckland CBD 1010, New Zealand

Email: privacy@snowball-x.com

Current customer-service channels: https://snowball-x.com/contact/

Please provide enough information for us to understand your request and, where necessary, verify your identity. Do not send passwords or unnecessary identity documents by unsecured email.

Office of the Privacy Commissioner

Website: https://www.privacy.org.nz/