Capital Investment Club

Privacy Policy

Public-facing privacy notice for data collection, use, sharing, retention, user choices, and security.

Last updated: 10/06/2024

Purpose

This Privacy Policy explains how Capital Investment Club collects, uses, shares, protects, and retains personal information when users access CIC websites, applications, marketplaces, pitch workflows, grant workflows, profile features, messaging, support, wallet-related features, and organization features.

Information We Collect

CIC may collect:

- Account information such as name, email address, phone number, username, password credentials, and authentication metadata.
- Profile information such as profile photo, role, bio, interests, expertise, specializations, qualifications, employment history, awards, public links, and visibility settings.
- Organization information such as organization name, members, roles, permissions, contact information, profile data, and governance activity.
- Pitch, grant, marketplace, project, assessment, application, and messaging content submitted through the platform.
- Wallet, transaction, ledger, fee, payment, contribution, investment, disbursement, and reconciliation-related records.
- Identity, KYC-adjacent, verification, support, and account recovery information where required for security, fraud prevention, compliance, or support.
- Device, browser, IP address, log, cookie, session, analytics, security, and usage information.
- Files, screenshots, or documents users provide for support, verification, grants, applications, assessments, or platform workflows.

How We Use Information

CIC uses information to:

- Provide, operate, secure, and improve the platform.
- Create and manage user and organization accounts.
- Support pitch, grant, investment, assessment, marketplace, wallet, messaging, and public profile workflows.
- Process user requests, applications, invitations, approvals, disbursements, support interactions, and notifications.
- Prevent fraud, abuse, unauthorized access, and security incidents.

- Perform verification, eligibility, compliance, audit, and operational reviews.
- Maintain platform integrity, logs, records, metrics, and evidence.
- Communicate with users about account activity, support requests, product changes, and policy updates.
- Meet legal, contractual, financial, security, and compliance obligations.

Public Profiles and Visibility

Users may have public profile features. If a profile is made public, logged-in platform users may be able to view the information the user has chosen or is allowed to make public. Users should not add information to public profile fields unless they are comfortable with that information being viewed by others.

How We Share Information

CIC may share information with:

- Other users or organizations as required by platform workflows and user visibility choices.
- Service providers that support hosting, security, analytics, email, notifications, payments, storage, customer support, and operations.
- Professional advisors, auditors, assessors, legal counsel, or compliance reviewers.
- Authorities, regulators, law enforcement, or third parties when legally required or needed to protect rights, users, platform security, or business integrity.
- Successors in connection with a merger, acquisition, financing, reorganization, or sale of assets.

CIC does not sell personal information as a standalone business model.

Cookies and Similar Technologies

CIC may use cookies, local storage, session storage, and similar technologies to support authentication, preferences, security, analytics, and platform functionality. See the Cookie Policy for more detail.

Data Security

CIC uses administrative, technical, and organizational controls designed to protect information. No system can be guaranteed completely secure, but CIC maintains policies and controls covering access, security risk, incident response, vendor review, secure development, evidence, and monitoring.

Data Retention

CIC retains information as long as needed for platform operations, support, legal obligations, financial records, fraud prevention, security, audit evidence, dispute resolution, and legitimate business purposes. Retention periods vary by data type and legal or operational need.

Data Retention Categories

CIC should maintain an internal retention schedule that distinguishes:

- Account profile records retained while the account is active and for a reasonable period afterward for support,

fraud prevention, security, and dispute resolution.

- Pitch, grant, marketplace, project, assessment, and application records retained for business history, contractual evidence, dispute resolution, audit, and platform integrity.
- Wallet, ledger, transaction, fee, investment, contribution, disbursement, and reconciliation records retained for legal, accounting, fraud prevention, audit, and financial integrity requirements.
- Messaging and support records retained for support continuity, safety, quality, investigation, and dispute resolution.
- KYC-adjacent or verification records retained only as required for security, compliance, fraud prevention, legal, operational, or provider requirements.
- Security logs retained for monitoring, incident response, fraud prevention, audit, and platform protection.

Legal Bases and Business Purposes

Where legal basis concepts apply, CIC may process information because:

- Processing is needed to provide the platform or perform requested services.
- Processing is needed for legitimate business interests such as security, fraud prevention, product improvement, customer support, platform integrity, audit readiness, and business operations.
- Processing is needed to comply with legal, contractual, accounting, tax, security, or regulatory obligations.
- Processing is based on consent where CIC specifically requests consent.

Sensitive Information

CIC should minimize collection of sensitive information. When sensitive data is necessary for verification, support, fraud prevention, security, or regulated workflows, CIC should restrict access, limit retention, and maintain an operational record of the purpose for collection.

Automated Processing and Profiling

CIC may use automated rules, eligibility checks, fraud signals, risk scoring, recommendation logic, or workflow automation to operate platform features. CIC should maintain human escalation or review paths for materially adverse platform decisions where practical and appropriate.

International Transfers

CIC may use cloud, support, analytics, payment, notification, security, or infrastructure providers that process data in different jurisdictions. CIC should use reasonable contractual and operational safeguards for cross-border processing where required.

Security Contact and Privacy Requests

CIC should maintain a published or support-routed method for privacy questions, account data requests, security concerns, and suspected misuse reports. Requests should be logged and dispositioned under the Data Subject Rights Policy and Incident Response Policy where applicable.

User Choices

Depending on the feature and applicable requirements, users may be able to:

- Update profile and account information.
- Change public profile visibility.
- Manage communication preferences.
- Request support with account or data questions.
- Request correction or deletion where legally and operationally permissible.

Some information may be retained when required for legal, financial, security, fraud prevention, audit, or dispute-resolution reasons.

Children

CIC is not intended for children. Users must meet the platform's eligibility requirements.

International Use

CIC may process information in jurisdictions where CIC or its service providers operate. Users are responsible for complying with laws applicable to their use of the platform.

Changes to This Policy

CIC may update this Privacy Policy from time to time. Material updates should be communicated through reasonable platform or website notice.

Contact

Questions about privacy or data handling should be sent through CIC's support or governance contact channels.