Capital Investment Club

Public Profile and User Content Policy

Visibility, user responsibilities, prohibited content, credential evidence, moderation, and reporting.

Last updated: 06/07/2026

Purpose

This policy defines expectations for public profiles, public content, and user-generated content on CIC.

Scope

This applies to user profiles, organization profiles, pitch pages, grant pages, marketplace listings, public profile links, assessments, comments, messages, uploads, external links, credentials, expertise, awards, employment history, qualifications, and other content submitted to CIC.

Public Profile Visibility

Users may be able to make profile information public. If public visibility is enabled, logged-in users may be able to view public profile information.

If public visibility is disabled, CIC should restrict profile visibility except where access is required for security, legal, administrative, or operational reasons.

Public profile controls must be explicit, user-controlled where appropriate, and reflected consistently across profile pages, public user pages, search surfaces, marketplace surfaces, grant and pitch workflows, messaging entry points, and profile cards.

Public Profile Data Rules

CIC should distinguish between:

- User-entered public profile information.
- Verification or KYC-adjacent status.
- Platform-calculated metrics.
- Private evidence submitted for verification.
- Administrative notes or support records.
- Sensitive financial, wallet, transaction, or application records.

Only information intended for public display should appear on public profiles. Evidence files, credentials, private verification documents, support notes, administrative comments, internal risk flags, moderation notes, and sensitive wallet or transaction details must not be displayed publicly unless a specific approved feature requires it and the user has appropriate notice.

User Responsibilities

Users are responsible for ensuring submitted content is accurate, lawful, and appropriate. Users should not publish confidential, private, misleading, infringing, or harmful content.

Prohibited Content

Users must not submit:

- Fraudulent or misleading claims.
- Unauthorized personal information.
- Confidential information without permission.
- Infringing content.
- Harassing, abusive, hateful, or threatening content.
- Malicious files or links.
- False credentials, qualifications, or organization affiliations.
- Content that violates law, platform rules, or third-party rights.

Credentials and Evidence

Users may submit credentials, qualifications, awards, certifications, links, and evidence. CIC may restrict public display of sensitive evidence while preserving it for verification or profile completeness.

Where CIC displays a credential, badge, score, verification marker, or experience metric, the display must be based on stored profile data, verified status, or clearly documented calculation logic. CIC should not display check marks, verified indicators, years of experience, assessment counts, badge totals, or trust labels that are inconsistent with the underlying profile state.

Calculated and Derived Fields

Public profile metrics must have an identified source and calculation owner. Examples include:

- Badge totals and earned dates.
- Profile completion or readiness.
- Assessment experience or specialties.
- Years of experience.
- Industries or areas of expertise.
- Followers/following counts.
- Verification and KYC status.

Derived values should be conservative and avoid overstating experience, verified status, or platform trust. If a value is not available, CIC should show a neutral empty state instead of invented or placeholder content.

Moderation

CIC may review, hide, remove, restrict, or report content when necessary to protect users, comply with law, enforce policies, prevent fraud, or maintain platform integrity.

Moderation actions should be proportionate, documented, and routed to an accountable owner. High-impact actions such as restricting a public profile, suspending an account, removing credentials, or escalating to legal/security require evidence and management visibility.

Reporting

Users should be able to report profiles or content where appropriate. Reports should be routed to a review queue and dispositioned with evidence of the outcome.

Report actions should be available to other users where appropriate, but users should not be able to report themselves. Report buttons should be discoverable without being visually disruptive to the main profile experience.

Public Profile Control Requirements

CIC should maintain controls so that:

- Public/private profile visibility is explicit.
- Private profiles are not visible to ordinary logged-in users.
- Users cannot follow, message, or report themselves.
- Profile verification indicators reflect actual verified status.
- KYC or verification status is not misrepresented.
- Public pages avoid exposing sensitive evidence or credentials unless intentionally public and appropriate.
- Report profile actions route to a disposition queue.
- Follow, message, report, and share controls respect self-view, private-profile, blocked-user, and permission states.
- Organization and user profiles display the correct image, name, role, and context.
- Public profile data is refreshed after profile edits and does not rely on stale static placeholders.
- External links are validated, labeled, and safe to open.
- Uploaded files shown publicly have approved type, preview, and sensitivity handling.

Content Review Triggers

CIC should review public profile or content behavior when:

- A new public profile field is introduced.
- A private field is reused on a public page.
- Badge, verification, or score logic changes.
- File upload, credential, or evidence display changes.
- Profile visibility or report-profile workflows change.
- A user reports inaccurate, misleading, or exposed information.
- A production incident suggests public/private data separation failed.

Notice and User Controls

Users should be able to understand which profile fields are public, private, or verification-only. Where practical,

CIC should provide previews of public profile appearance and clear controls for changing visibility.

Moderation Disposition

Profile and content reports should be dispositioned as:

- No action.
- User warning.
- Content hidden.
- Content removed.
- Profile visibility restricted.
- Account restricted.
- Escalated to security, legal, support, or leadership.

Appeals and Correction

Where appropriate, users should be able to request review of moderation actions or correct inaccurate profile information.

Correction requests involving public profile inaccuracies should be prioritized when the inaccurate field could affect trust, hiring, funding, assessment selection, investment decisions, grant eligibility, or user reputation.

Evidence

Required evidence:

- Report records
- Moderation decisions
- Content removal records
- Appeal or dispute records where applicable
- Profile visibility setting records
- Public/private field mapping
- Derived-field calculation references
- Report disposition records
- Public profile regression test evidence
- Moderation queue records

Review

This policy must be reviewed at least annually.