



Clean Play Standards 1.0: Mobile Games

Nine mandatory, auditable requirements for games built to entertain, not exploit

Clean Play Standards

August 6, 2026



Contents at a glance

- - 1. Purpose
- - 2. Scope
- - 3. Names and public designations
- - 4. Decision rule
- CPS-01: No Disruptive Ads
- CPS-02: No Tracking
- CPS-03: No Forced Accounts
- CPS-04: No Loot Boxes
- CPS-05: No FOMO Mechanics
- CPS-06: No Premium Currencies
- CPS-07: No Pay-to-Win
- CPS-08: No Hostile Notifications
- CPS-09: No Hidden Subscriptions
- - 14. Third-party service rule
- - 15. Audit and credential lifecycle
- - 16. Badge integrity
- - 17. Exceptions, appeals, and changes
- - 18. References and alignment
- - 19. Legal and status notice



Document code: CPS-MG-1.0

Status: Public working draft

Draft date: August 6, 2026

Publisher: Clean Play Standards, an independent public-interest initiative preparing nonprofit incorporation

Core principle: Mobile games should be built to entertain, not to exploit.

1. Purpose

This standard turns nine player-respect commitments into auditable requirements for consumer-facing mobile games. It is stricter than the minimum rules of major app stores. A Clean Play decision is not a legal opinion, security warranty, age rating, government approval, or guarantee that a game is free of every defect.

2. Scope

- Applies initially to named mobile games on iOS, iPadOS, and Android.
- The certification covers the product, platforms, versions, regions, monetization configuration, and service inventory identified in the public registry.
- All nine commitments are mandatory. A requirement may be marked not applicable only when the feature truly does not exist.
- Child-safety and accessibility guidance are strongly recommended companion guides, but they are not part of the nine-condition pass/fail decision in Standard 1.0.
- A credential normally lasts 12 months. Material changes to ads, tracking, accounts, economy, notifications, subscriptions, or third-party SDKs require notice and may trigger re-review.

3. Names and public designations

- **Clean Play Standards** - the organization and standards program.
- **Clean Play Standards 1.0: Mobile Games** - the controlled, auditable rule set.
- **Clean Play Certified** - the single certification result and certification mark for a named product scope with an Active, unexpired, unrevoked registry credential.

Applications, reviews, remediation, decisions, suspension, expiry, and revocation are workflow or registry states. They are not separate public programs, awards, memberships, tiers, or badges.

4. Decision rule

A product passes only when every applicable commitment passes. There is no compensating score: strength in one area does not cancel a failure in another. Documentation gaps must be resolved before a badge is issued. The certification decision is recorded before any maintenance contribution or waiver is requested, so payment cannot buy or influence the result.

CPS-01: No Disruptive Ads

Requirement: Advertising must not interrupt play, track people, trick taps, or hold progress hostage.

Why it matters: Players should be able to use a game without having their attention seized or their behavior profiled for advertising.

Prohibited examples

- Third-party advertising network SDKs or mediation layers.
- Persistent banner ads over gameplay or core navigation.
- Surprise interstitials, pop-ups, or ads inserted after failure, level completion, launch, or return from background.



- Forced or progress-gated video advertisements, including rewarded ads required for normal progression.
- Deceptive close controls, fake gameplay, accidental-tap layouts, or ads visually disguised as game controls.
- Behaviorally targeted, cross-app, or user-profiled advertising.

Permitted examples

- A clearly labeled, static house promotion for another product from the same developer, placed in a menu and not during play.
- A direct sponsorship or product placement baked into the game with no ad SDK, user-level reporting, dynamic targeting, or interruption.
- A straightforward premium-unlock, expansion, soundtrack, or tip/support option.
- Storefront links the player deliberately opens.

Reasonable caveat

Standard 1.0 does not allow network-served rewarded ads, even when the button is optional, because the network and measurement layer usually conflicts with the tracking rule. A future limited-ad profile could be considered through public rulemaking, but it is not part of this standard.

Minimum evidence

- Complete SDK/dependency inventory.
- Screenshots or video of menus, failure states, level transitions, and purchase screens.
- Network traffic sample or privacy report showing no ad endpoints.
- Written list of all sponsors, house promotions, and outbound commercial links.

Pass test

Reviewers can complete a representative play session without receiving a network ad, forced commercial interruption, deceptive ad control, or progress gate tied to advertising.

CPS-02: No Tracking

Requirement: No advertising tracking, behavioral profiling, cross-app surveillance, or unnecessary telemetry.

Why it matters: A game should not turn a player into a behavioral data product. Reliability and security diagnostics may exist only when tightly limited.

Prohibited examples

- Advertising identifiers, cross-app identifiers, device fingerprinting, or data-broker enrichment.
- Behavioral profiles used for advertising, monetization pressure, churn manipulation, or personalized compulsion.
- Third-party analytics that may independently use data or combine it across customers.
- Session replay, screen recording, keystroke capture, or raw interaction streams.
- Collection of precise location, contacts, photos, microphone data, or other sensitive data without a necessary player-requested feature.
- Indefinite event-level logs or collecting data merely because it might become useful.

Permitted examples

- On-device logs that remain on the device unless the player deliberately shares them.
- Platform-provided crash and performance diagnostics configured to minimize data.
- First-party operational counters that are aggregated, short-lived, documented, and not linked across products.
- Security, fraud-prevention, and abuse-prevention records limited to the purpose and retention period.
- Opt-in research with a separate clear consent and an easy withdrawal path.



Reasonable caveat

A third-party processor may be used for hosting, payments, crash handling, email, or security when it acts only on documented instructions; has no right to advertise, profile, sell, or independently reuse the data; receives the minimum fields; uses appropriate security; and is covered by a written processing agreement. The reviewer evaluates the configuration and contract, not merely the vendor name.

Minimum evidence

- Data inventory and flow diagram.
- SDK/service inventory with purposes, fields, retention, and processor terms.
- Privacy manifest/Data Safety disclosures and storefront privacy answers.
- Sample logs or analytics events with identifiers redacted.
- Deletion and retention configuration.

Pass test

Every collected field has a necessary, disclosed purpose; prohibited identifiers and profiling are absent; permitted diagnostics are minimized, secured, and time-limited.

CPS-03: No Forced Accounts

Requirement: Basic play must not require an unnecessary sign-up, profile, social login, or email address.

Why it matters: Players should not have to surrender identity information to use a game whose core function can work without it.

Prohibited examples

- Blocking first play behind registration when the game can function locally.
- Requiring email, phone number, or social login for basic or offline play.
- Making guest mode materially worse solely to force registration.
- Requiring marketing consent as a condition of creating an account.
- Preventing account deletion or making it harder than account creation.

Permitted examples

- Guest or local play by default.
- An optional account for cloud saves, cross-device sync, online multiplayer, purchases, parental controls, moderation, or user-requested social features.
- Age-appropriate identity or parental steps where legally necessary.
- A device-local profile that is not transmitted and does not require contact information.

Reasonable caveat

When an online feature genuinely requires identity, the requirement must be limited to that feature, explained before collection, and accompanied by deletion and recovery controls. "No forced accounts" does not mean "no accounts under any circumstances."

Minimum evidence

- First-run and guest-mode screen recording.
- Feature matrix showing what works without an account.
- Account data fields and purpose list.
- Deletion flow and recovery process.



Pass test

A reviewer can access the game's basic promised experience without creating an account unless the entire product is inherently account-based and the necessity is documented and accepted in scope.

CPS-04: No Loot Boxes

Requirement: No paid randomness, gacha, mystery purchases, paid spins, or gambling-like reward systems.

Why it matters: Players should know what they are buying. Payment must never purchase a chance at an unknown reward.

Prohibited examples

- Paid loot boxes, gacha pulls, mystery crates, paid card packs, paid wheels, or keys for random chests.
- Random rewards purchased directly or indirectly with paid currency.
- Paid acceleration that materially increases access to random valuable rewards.
- Cash-out, resale, wagering, or gambling-like systems involving real or paid value.

Permitted examples

- Random level generation, procedural content, or chance events that are not sold.
- Random gameplay drops earned only through ordinary play with no purchase route, cash value, paid boost, or monetized key.
- A clearly identified fixed bundle where every included item is shown before purchase.

Reasonable caveat

Publishing odds does not make a paid-random system Clean Play compliant. If paid value can reach the random outcome through any chain of conversion, the rule is failed.

Minimum evidence

- Complete in-app purchase catalog.
- Economy diagram showing every source and sink of value.
- Video of reward-opening flows.
- Server configuration or item tables where relevant.

Pass test

No payment, paid token, subscription benefit, advertisement, or purchasable accelerator can produce or materially increase a randomized reward.

CPS-05: No FOMO Mechanics

Requirement: No fake scarcity, streak punishment, energy pressure, or artificial urgency designed to compel return visits or spending.

Why it matters: Games may be engaging without manufacturing anxiety about stopping, missing out, or losing accumulated value.

Prohibited examples

- Daily-login streaks that remove accumulated rewards, status, or benefits when a day is missed.
- Energy systems or timers engineered primarily to interrupt play and sell waiting relief.
- Fake or repeatedly resetting countdowns.
- Paid items presented as scarce when the scarcity is artificial or undisclosed.
- Expiring paid content or purchases that disappear without a necessary service reason.



- Aggressive event schedules designed to make healthy breaks costly.

Permitted examples

- Optional daily or weekly challenges with no loss, punishment, compounding disadvantage, or spending pressure.
- Honest seasonal events with published dates, reasonable notice, and no deceptive scarcity.
- Rotating free content that returns or offers an equivalent non-pressure path.
- User-created reminders and calendars.

Reasonable caveat

Limited-time content is not automatically prohibited. The audit asks whether timing is truthful, proportionate, non-punitive, and separable from spending pressure. A genuine live event may end; a fabricated emergency sale may not.

Minimum evidence

- Event calendar and offer history.
- Streak, timer, energy, and reward configuration.
- Screenshots of countdowns and scarcity claims.
- Design notes explaining the purpose of time limits.

Pass test

Taking a normal break does not destroy accumulated value, create a material competitive penalty, or expose the player to deceptive urgency or a monetized wait.

CPS-06: No Premium Currencies

Requirement: Real-money prices must stay visible; purchasable gems, coins, tokens, and odd bundles may not obscure cost.

Why it matters: Players should understand the actual price of every purchase without currency conversion, leftovers, or bundle arithmetic.

Prohibited examples

- Selling gems, crystals, coins, credits, tokens, or similar intermediate currency.
- Using multiple currencies to separate spending from real-world value.
- Odd denomination bundles that predictably leave unusable balances.
- Bonus-currency claims that obscure unit price or create urgency.
- Routing subscriptions, power, loot boxes, or consumables through a paid currency.

Permitted examples

- Direct prices in the user's storefront currency.
- Earned-only score, coins, or crafting materials that cannot be purchased, exchanged for paid value, or accelerated with payment.
- One-time full-game unlocks, fixed expansions, cosmetics, and clearly priced content.

Reasonable caveat

A currency is treated as premium if money or a paid entitlement can increase it, even if it can also be earned. Platform store balances and gift cards are outside the game's own economy and are not counted as an in-game premium currency.

Minimum evidence

- Purchase catalog and screenshots showing local-currency prices.



- Economy sources/sinks diagram.
- Configuration proving gameplay currencies are not purchasable.

Pass test

A player can identify the exact real-world price of each purchase at the decision point without converting an in-game currency or consuming a prepaid balance.

CPS-07: No Pay-to-Win

Requirement: Payment must not buy power, rank, competitive advantage, or relief from frustration deliberately engineered for sale.

Why it matters: Money should not determine who wins or whether a deliberately unpleasant design becomes tolerable.

Prohibited examples

- Purchasable stats, weapons, characters, boosts, extra lives, speedups, or matchmaking advantages that affect competitive outcomes.
- Selling progress skips for grind or difficulty intentionally created to drive purchases.
- Paid retries, revives, or energy that materially alter progression or leaderboard opportunity.
- Subscription-only power or resource multipliers.

Permitted examples

- Cosmetic items with no gameplay effect.
- A transparent full-game unlock, fixed expansion, soundtrack, art book, or additional story content.
- Separate content packs that do not disadvantage owners of the base game in shared competition.
- Free difficulty, accessibility, assist, and pacing options.

Reasonable caveat

Single-player games can still fail this rule when frustration is deliberately engineered and then sold back as relief. Paying for additional authored content is different from paying to bypass manipulated friction.

Minimum evidence

- Purchase-effect matrix.
- Competitive balance and matchmaking design.
- Progression curves before and after purchases.
- Video of purchase prompts near failures or resource depletion.

Pass test

A paying player receives no gameplay advantage over a nonpaying player in shared competition, and no purchase is needed to escape intentionally monetized frustration.

CPS-08: No Hostile Notifications

Requirement: Notifications must be useful, requested, truthful, easy to stop, and free of guilt or manufactured urgency.

Why it matters: A player's device should not be used to pressure, shame, alarm, or repeatedly pull them back into a game.

Prohibited examples

- Messages claiming a character is lonely, hurt, disappointed, or waiting because the player stopped.
- False urgency, expiring-reward threats, streak-loss warnings, or misleading "someone needs you" language.



- Marketing notifications enabled without a clear opt-in.
- Repeated permission prompts after refusal.
- Notifications sent at unreasonable hours without user control.

Permitted examples

- Transactional notices about purchases, security, account changes, or service interruptions.
- User-scheduled reminders.
- Opt-in event announcements with truthful dates and no punishment.
- Parental, safety, moderation, or multiplayer notices necessary for a requested feature.

Reasonable caveat

A notification may be important and still fail if its wording manipulates emotion or if users cannot control the category. Critical security notices may be sent without marketing consent, but should be narrowly limited.

Minimum evidence

- Notification catalog with trigger, audience, default, wording, and category.
- Permission prompt and settings screen.
- Quiet-hours behavior and opt-out test.

Pass test

All nonessential notifications are off until affirmatively enabled, every category can be disabled, and no message uses guilt, deception, or artificial urgency.

CPS-09: No Hidden Subscriptions

Requirement: Recurring charges must be obvious before purchase, easy to manage, and free of cancellation obstruction.

Why it matters: A subscription should continue only because the player knowingly values it, not because renewal or cancellation was concealed.

Prohibited examples

- Burying the recurring price, billing period, renewal, trial conversion, or material limits.
- Displaying a monthly equivalent more prominently than the actual annual charge.
- Preselected subscription options or confusing one-time and recurring offers.
- Making cancellation materially harder than sign-up.
- Requiring a support request, guilt flow, maze, or repeated retention offers before cancellation.
- Continuing to describe expired trials or discounts as urgent when they routinely reset.

Permitted examples

- A clearly labeled monthly or annual subscription with the full amount and renewal cadence shown before confirmation.
- A direct link to platform subscription management.
- A renewal reminder, especially before a trial converts or a long annual term renews.
- Immediate cancellation with access continuing through the already-paid period.
- One-time purchases presented separately from subscriptions.

Reasonable caveat

Platform billing systems control the final cancellation mechanics. The developer must provide the clearest available route, accurate disclosures, restoration, and responsive support. Clean Play Standards



applies the same transparency rule to its own certification-maintenance contribution and any future paid service.

Minimum evidence

- Purchase and trial screens.
- Store product metadata.
- Cancellation and restoration recording.
- Customer support and refund instructions.

Pass test

A reasonable user can identify the recurring amount and cadence before purchase and reach the platform cancellation control from the app or service without obstruction.

14. Third-party service rule

A third-party company is not automatically good or bad. The audit examines what the service actually receives, what it is permitted to do, how long it retains data, whether it can combine data across customers, and whether the game can function without an invasive SDK. Advertising networks, cross-app attribution, data brokers, and behavioral profiling fail by category. Hosting, payments, email, security, and limited diagnostics can be permitted when they act only as controlled service providers.

15. Audit and credential lifecycle

1. Applicant submits the product, service inventory, store links, and evidence.
2. Clean Play performs conflict screening and completeness review.
3. A reviewer tests the build and evidence against every applicable pass test.
4. The applicant receives findings and may remediate them.
5. A separate final decision records pass or fail.
6. After a pass, the applicant may activate the \$12 annual certification-maintenance contribution or receive a written waiver.
7. Clean Play issues a product-specific signed credential and public registry entry.
8. Complaints, material changes, expiry, or failure to maintain required terms can cause review, suspension, expiry, or revocation.
9. Renewal requires a fresh attestation and risk-based review at least annually.

16. Badge integrity

- A badge image alone proves nothing; it must link to a live Clean Play verification page.
- Each credential identifies the issuer, product, platforms, standard version, audit date, expiry, status, and public evidence summary.
- Credentials are digitally signed and include a revocation/status endpoint.
- Copying an image, altering its status strip, or using it for an unlisted product is prohibited.
- “Clean Play Certified” means only that the exact published product scope passed this private standard and the registry status is Active; it is not government, Apple, Google, legal, safety, security, accessibility, child-safety, or quality approval.

17. Exceptions, appeals, and changes

- Standard-defined permitted cases are not waivers.
- A reviewer may not privately waive a mandatory rule.
- Applicants may appeal factual or procedural errors to a reviewer not responsible for the original decision when staffing allows.
- Material rule changes require versioning, a change log, and a transition period.



18. References and alignment

Clean Play is informed by consumer-protection, privacy, child-well-being, accessibility, and credential standards. The source mapping in this kit identifies the relationship without claiming endorsement by those organizations.

19. Legal and status notice

This is an attorney-review draft. Clean Play Standards is not yet represented as an incorporated or IRS-recognized tax-exempt organization. The standard does not replace legal compliance, platform review, security testing, accessibility evaluation, age-rating obligations, or professional advice.

Formation-stage working material. Adoption, legal review, deployment, staffing, testing, and real records are required before production certification.