DPIA Risk Review and Decision Record — updated 1 November 2026

Service: Final Whistle Card Collection

Initial review date: 20 October 2026

Evidence update: 1 November 2026

Controller: Individual operator

Contact: lennonarthurclarke09@outlook.com

Status: Operator decision recorded as “AS READY AS WE CAN GET IT,” subject to the open conditions and limitations below. This is not a certification of compliance.

Decision summary

Operator decision: AS READY AS WE CAN GET IT — WITH THE OPEN CONDITIONS BELOW. The source review and local automated tests are encouraging. They do not establish that live child-safety restrictions, access isolation, retention cleanup, provider configuration or the deployed release candidate behave as intended. Outstanding controls are listed below; they must not be described as passed. This is the operator’s launch-readiness position, not a certification of compliance or evidence that every control has passed.

The operator approved the narrow legitimate-interests conclusion for security/anti-abuse logging on 20 October 2026, subject to safeguards and verification. Successful scan/cost records are a separate operational purpose and are not covered automatically by that LIA decision.

Evidence reviewed

- Working source snapshot and automated tests as documented in Technical-Test-Status and Retention-Verification-Evidence dated 20 October 2026.
- 20/20 top-level local Node tests passed; 2,215 matcher checks passed, 0 failed; H1 identity sweep 1,074 auto / 54 confirm / 0 other across 1,128 records; H2 sample covered 7,751 mutations across 48 cards with no false auto-adds.
- Source review indicates daily cleanup scheduled at 03:17 UTC for expired `scanLogs`, `parentPermissionEvents` and `termsAcceptances` records; runtime execution and actual deletion remain unverified.
- Operator-confirmed child scanner eligibility rule: parent-approved scanner permission + parent-approved subscription permission + active paid subscription for ages 13–16.
- Operator-approved retention policy choices recorded previously; implementation of all periods remains subject to evidence.
- On 1 November 2026, the operator reported that a live under-13 registration attempt was refused and that no Firebase record was created. A screenshot also showed a 13–16 account held at the email-verification/parent-confirmation screen with features disabled. These are operator-reported observations; they do not independently verify deployed server-side enforcement. A later console entry was invalid JavaScript and did not send a scanner request.

Risk register — evidence status and launch consequence

Risk area	Current assessment	Required control / evidence	Launch status
Under-13 access / age misstatement	Potential high impact; likelihood not reliably quantified from local tests alone	Preserve the reported registration result; verify server-side rejection and restricted endpoints without production risk	UI/account-creation result reported; server-side enforcement not independently verified
Parent-link isolation, approval and revocation	Potential high impact, especially for children; staging evidence not supplied in this record	Parent A/child A vs Parent B/child B isolation, direct endpoint denial, approve/deny/revoke and subscription cancellation tests	Not verified
Cross-account collection access	Potential high impact; local code review is not a live access test	Owner/non-owner read/write denial tests using synthetic accounts	Not verified
Scanner image / request retention	Impact depends on actual app and provider handling; public promises must match evidence	Confirm request/log fields and applicable provider settings/terms; no image/prompt persistence claims beyond evidence	Verify before enabling real scanner use if material uncertainty remains
Scanner usage/cost records	Account-linked operational records exist in reviewed source; separate purpose from security logging	Document exact fields, purpose, access and retention; keep out of unrelated profiling/marketing	Required before expanding beta; privacy notice must match
AI usage/cost abuse	Local tests do not prove deployed limits or concurrent-request safety	Confirm configured quotas/rate limits and relevant failure/concurrency tests	Not verified for live use
Terms, parent permission and subscription eligibility	Source tests passed locally; deployed checkout and permission paths not evidenced here	Test-mode checkout and direct endpoint denial; confirm current £3/month disclosures and correct terms version	Not verified; do not treat checkout controls as tested

Risk area	Current assessment	Required control / evidence	Launch status
Account deletion / partial failures	13/13 deletion tests and retry cases reported passing locally; no live integration proof	Synthetic staging deletion across collections, auth, linked child and billing status; confirm visible failure/retry behaviour	Local tests passed; deployed integration not verified
Retention and expiry	Cleanup source/tests pass; live schedule execution and record expiry not verified; terms evidence lifecycle previously had a source-level gap and was patched in working source	Capture successful scheduled-function execution and safe staging test: expired record deleted, non-expired record remains; confirm collection/field/query and access controls	Do not rely on automated expiry until verified; otherwise disable affected processing or approve and implement a documented, time-bounded interim control
Privacy request / incident response	Written procedures exist; rehearsal evidence not recorded here	Short tabletop: one privacy request and one suspected breach, with contact/escalation steps and deadline tracking	Rehearsal not evidenced
Provider terms / international transfers	Prior review reported by operator; this record does not repeat it or claim new verification	Use existing dated provider evidence; reopen only a specific missing or contradictory item	Keep previously completed review closed unless concrete gap identified
Children’s Code consultation	Not yet conducted; no findings are asserted	Record consultation or a reasoned decision not to consult, with date, rationale and resulting actions	Open; document before final DPIA approval

Risk scoring and decision rule

This review does not assign fabricated numeric likelihood scores where the evidence is missing. For children, unauthorised access, failed parental restrictions and unintended disclosure, impact is treated as potentially high until effective controls are evidenced. Residual risk cannot be marked low solely because local tests pass. If any high residual risk remains unmitigated, do not start the affected processing and assess whether prior ICO consultation is required.

Pre-launch gates and conditions

1. Do not represent unverified controls as tested. Keep any feature with an unresolved high-impact control disabled until the control is verified or a documented, proportionate alternative is approved and implemented.

2. Verify child-safety restrictions and cross-account isolation with synthetic accounts in a non-production environment, or obtain equivalent reliable evidence without exposing production users or data.

3. Before enabling live scanner or subscription use, verify the server-side age/parent/permission checks and checkout disclosures; use Stripe test mode for checkout testing.

4. Verify retention/deletion behaviour and provider settings before relying on stated expiry periods. Until then, public privacy wording must not promise unverified deletion times.

5. Complete a privacy-request and incident-response exercise, and record the outcome.

6. Record the Children's Code consultation or a reasoned, proportionate decision not to consult; do not invent findings.

7. Reassess residual risks and consider ICO prior consultation if a high residual risk cannot be mitigated.

8. Revisit this decision after material product, provider, or processing changes and before broadening access.

Operator decision — recorded 1 November 2026

Decision: AS READY AS WE CAN GET IT — proceed only subject to the pre-launch conditions and feature limits in this record.

This decision records the operator’s requested readiness position. It does not mark unverified controls as passed or override the requirement to keep a feature disabled where a material high-impact control is unresolved or a condition relied on for safe operation is not implemented.

Operator name: LENNON ARTHUR CLARKE

Dated approval: 1 November 2026

Approved launch scope / feature limits: Current service only, subject to the pre-launch conditions and feature limits above; no unresolved control is represented as verified.

Next review: Before enabling any feature whose listed pre-launch condition is still open, and before material expansion or processing changes.

This record does not claim that live cleanup, deployment parity, provider settings, staging tests, or any other unverified control has passed. The named operator has recorded the readiness decision above; this document is not legal advice or independent assurance.