Final Whistle Card Collection

Retention and Deletion Schedule

Updated 20 October 2026

Purpose and status

This schedule records the operator-selected retention periods and the status of implementation. Periods are policy choices, not universal statutory defaults. The current website source includes an application-managed daily cleanup function. Local automated tests passed on 20 October 2026 (20/20 top-level tests; 2,215 matcher checks passed), but live scheduled execution and deletion outcomes have not yet been verified. The schedule therefore does not claim that automatic deletion is operational.

Record type	Selected period / handling	Implementation status
Scanner logs	Maximum 30 days from the relevant expiry timestamp.	Source includes daily scheduled cleanup; live run/deletion evidence pending.
Platform/authentication security logs	90-day review window; minimise and restrict access.	Provider-specific retention and actual fields require confirmation.
Support and privacy requests	24 months after closure, unless a documented reason requires a limited exception.	Procedure exists; ensure operational records follow the schedule.
Terms-acceptance evidence	Minimum restricted evidence for up to 2 years after account closure.	Account-closure source minimises record and sets deleteAfter; live deletion pending.
Parental-permission evidence	Up to 2 years after relevant withdrawal/account-closure trigger, as applicable.	Source schedules deleteAfter; live deletion pending.
Personal-data incident records	Risk-based, documented retention and periodic review.	Maintain a reason and access restriction for each retained record.
Aggregate scanner-usage totals	Retain only while useful; review at least annually.	After account closure, retained card/duplicate statistics must be anonymous and unlinked to the former account. Verify effective anonymisation.
Backups and recovery data	Firebase backup/PITR and external backup retention are managed separately; deleted live records may remain until the configured backup/recovery period expires.	Do not assume live-database cleanup immediately removes backup copies. Confirm provider settings separately.

Required evidence before marking deletion operational

• A dated Netlify execution log for the scheduled retention-cleanup function.

• Safe test evidence that an expired record is deleted and a non-expired record is preserved.

• Confirmation that live Firestore queries, indexes, and service access work as intended.

• Separate review of provider-side and backup/recovery retention.

Contact: lennonarthurclarke09@outlook.com