← Back to Final Whistle

Privacy Policy

Last updated: 18 October 2026

This Privacy Policy describes how Final Whistle Card Collection handles personal information. Retention periods and safeguards are set out below; where a technical deletion process is still being verified, this page does not claim that the process has been proven operational.

Who operates the service

Final Whistle Card Collection is an unofficial fan-made collection tracker. It is not affiliated with or endorsed by any league, club or card manufacturer. The service is operated by Lennon Arthur Clarke as a sole trader. Contact: lennonarthurclarke09@outlook.com .

Information we process

Account details, such as your email address and Firebase user identifier, to create and secure your account.

Collection information you enter, including cards owned, numbered cards, hobby checklist progress and relevant collection-management data.

Operational scanner-usage summaries and related diagnostic information to monitor system usage and reliability. The current usage-summary note says successful scans are not individually logged and that counts are recorded from the deployment of the relevant change onward; the exact stored fields and whether any totals can be linked to an account must be verified before this policy is treated as final.

Subscription and billing identifiers/status received from Stripe. Card payment details are handled by Stripe, not stored by this website.

Date of birth and age band, used to apply age restrictions and determine whether parental controls are required.

For users aged 13–16, the parent’s email address, parent-account link, feature permissions and feature-request decisions. A parent must use a separate adult account with a verified email address.

Card photos and AI scanning

If you choose to use the optional AI scanner, the image you submit is sent from the browser to our secure server and then to OpenAI to extract card details. The website's scanner function is designed not to save the image in our database or usage logs. OpenAI processes the image under its own applicable terms and privacy/data-processing commitments. Do not scan images containing unrelated personal or sensitive information.

Why we use information

We use information to operate your account and collection, provide optional scanning, administer subscriptions, prevent abuse, troubleshoot errors, protect the service and meet legal obligations. We do not sell personal information.

Services that process information

The service uses Firebase for authentication and database hosting, Netlify for website hosting/server functions, Stripe for subscription payments and OpenAI for AI scanning. These providers may process data in countries outside the UK; their applicable safeguards and terms should be reviewed before launch.

Privacy and access controls

Your collection is intended to be private to your account. The two original accounts have a specifically configured legacy sharing arrangement. New accounts do not inherit that access. Server-side permissions and Firebase security rules are required for this promise to hold.

Age rules and parental controls

Users under 13 cannot register. Users aged 13–16 must provide their own email address and a parent’s email address, verify their own email, and wait for the parent to confirm through a separate adult account with a verified email. Manual card entry, the AI scanner and subscription access are disabled by default for these users. A parent can approve or reject feature requests, change permissions later, and delete a linked child account. Users aged 17 and over use the website without these parental restrictions.

We use the date of birth to calculate the age band and transition accounts out of parental controls when the user turns 17. The date of birth is stored in Firebase for that purpose. A parent’s email and account link are cleared when the child account transitions out of parental controls. Feature-request notifications by email are sent only when the optional SMTP email configuration is enabled; otherwise, requests are available in the parent dashboard.

An email verification link confirms access to an email inbox; it does not independently prove a person’s legal relationship to a child. The parent-link process checks that the adult account’s verified email matches the parent email supplied at registration. This is a proportionate control but not a high-assurance identity or guardianship check.

Retention

When an account is deleted, we intend to remove personal account and collection records that are no longer needed, subject to limited records we must or can lawfully retain. We may keep card-count and duplicate-count statistics only in anonymous form, without an account link, where the figures cannot reasonably be linked back to the former user. If effective anonymisation cannot be confirmed, the figures must not be treated as anonymous. Retained records are reviewed at least annually, and statistics that are no longer useful are deleted.

The retention schedule sets a maximum of 30 days for scanner logs. The source includes an application-managed scheduled cleanup function for expired records. Local automated tests passed on 20 October 2026, but the scheduled function’s live execution and deletion outcomes have not yet been verified; an expiry timestamp alone does not confirm deletion.

Our Firebase database has daily scheduled backups configured for a 28-day retention period and point-in-time recovery configured for a 7-day period. Information deleted from the live database may remain in existing backups or recovery data until the relevant retention period expires.

The retention schedule also sets a 90-day review window for authentication/platform security logs and 24 months after closure for support and privacy requests. Terms-acceptance and parental-consent evidence is proposed to be retained for two years after account closure or consent withdrawal, as applicable. Personal-data incident records are retained according to risk, with documented reasons and periodic review. Daily and monthly aggregate scanner-usage totals may be retained while useful, subject to an annual usefulness review and deletion if no longer useful. After account deletion, only anonymous card-count and duplicate-count totals without account links may be retained; effective anonymisation must be verified. These periods are the selected retention policy; actual fields, storage links and live deletion behaviour must be verified, and specific legal obligations or documented disputes may require limited exceptions.

Payment and accounting information may be retained for longer where required by law or necessary for accounting and dispute-resolution purposes. Deletion from the live database does not necessarily immediately remove every copy held in backups or by service providers. Provider-specific retention arrangements may also apply.

Your choices and rights

Depending on the circumstances, UK data-protection law may give you rights to access, correct, delete, restrict or object to certain processing, and to complain to the Information Commissioner's Office. To ask a question or request deletion, contact lennonarthurclarke09@outlook.com . A self-service account-deletion feature should be enabled before public launch.

Children

Registration is blocked for children under 13. For users aged 13–16, parental confirmation and feature permissions apply as described above. We aim to collect only the parent details needed to establish the link and manage permissions. If you believe an account has entered an incorrect age or a child has provided information improperly, contact the operator.

Changes

We may update this policy as the service changes. The latest version will be published on this page.