Legal and Compliance Checklist — Public Copy

Final Whistle Card Collection — Legal & Compliance Handover

1. Project overview

I run **Final Whistle Card Collection**, a football-card collection website:

https://finalwhistlecardcollection.netlify.app/

• Business structure: sole trader.

• Operator: Lennon Arthur Clarke.

• Contact email: lennonarthurclarke09@outlook.com

• Hosting: Netlify.

• Authentication: Firebase Authentication, using email/password and password reset.

• Database: Firestore, storing collection information and scan logs.

• AI card scanner: uses the OpenAI API to identify football cards.

• Payments: Stripe subscriptions costing £5 per month.

• Intended audience: football-card collectors, including younger users aged 13–17.

Important: I do not want to publish my home address because it is residential. We agreed to leave the question of public business address details unresolved until we determine a suitable approach.

2. What I am trying to achieve

I want to make the website legally compliant for UK users, including data protection, privacy, subscriptions, cookies, consumer rights and younger users.

I want practical, step-by-step guidance in plain English. Work through the checklist one issue at a time rather than overwhelming me with everything at once. Explain what I actually need to do, distinguish legal requirements from good practice, and avoid claiming something is legally required unless that is supported.

I want to keep the paperwork manageable, but I do not want to overlook important legal obligations.

This is a compliance project, not a request for a generic set of templates. Recommendations should account for how the website actually works.

3. Important technical findings

The following findings came from inspecting a ZIP of the website's code. They should be reverified against the current version before being treated as confirmed.

Authentication and data

• Firebase Authentication supports email/password accounts and password resets.

• Firestore stores users' collection data and scan logs.

• The site may store collection details, duplicate-card records, checklist progress and scanner results.

• Account deletion needs to be tested to establish whether associated Firestore data is deleted as well.

• Account deletion and the handling of related Stripe subscriptions have not been fully verified.

AI card scanner

• The scanner code was located at `netlify/functions/scan-card.js`.

• It sends card images as Base64 image data to the OpenAI Chat Completions API.

• The inspected implementation did not appear to use the OpenAI Files API.

• The intention is not to save submitted card images in the collection database or scan logs. However, this does not automatically mean the images are not processed or retained by OpenAI, Netlify or other relevant systems.

• The exact model name in the code needs verification; a previously observed name, `gpt-6-luna`, looked suspicious and should not be assumed to be a valid model.

• I have said that my OpenAI data-sharing settings are all enabled because I want to retain access to complimentary/free tokens. Verify the actual account settings, model eligibility and current OpenAI policies before explaining what this means. Do not promise that every input or output is used for training or that every request qualifies for free tokens.

Scan-log retention

• Earlier code inspection suggested scan-log records receive an `expireAt` timestamp approximately 365 days in the future in several places.

• This does not prove records are automatically deleted. Firestore TTL must be configured and verified, and actual deletion behaviour should be tested.

• The intended retention period and what happens to expired records need to be documented accurately.

Cookies and browser storage

A preliminary code audit of `final-whistle-settings-and-tutorials(1).zip` found:

• `localStorage` is used for scanner preferences, including the selected camera and auto-scan preference.

• `sessionStorage` is used to remember whether the user has seen the tutorial during the current browser session.

• Firebase Authentication may use browser storage to maintain sign-in state, depending on its configuration.

• Firebase configuration contained a Google Analytics measurement ID, but no Analytics SDK import was found in the code inspected.

• No explicit Google Analytics SDK, Meta Pixel, Hotjar or similar tracking integration was found in the files inspected.

• Google Fonts, Firebase, Netlify and Stripe are used. Their presence alone does not prove that they set cookies or require consent, but their actual behaviour needs checking.

Crucial limitation: This was a code inspection, not a complete live-browser audit. Runtime behaviour, third-party cookies, redirects, Stripe checkout and any scripts loaded dynamically still need checking.

4. Younger users and the Children's Code

I want younger football-card collectors to be able to use the website. I do not want to introduce unnecessary paperwork, but I need to understand my obligations.

Current situation:

• There is no known age-verification system.

• There is no known parental approval process for subscriptions.

• Users can subscribe for £5 per month if they have a valid payment card and sufficient funds.

• The site may be accessed by children aged 13–17.

We discussed the UK's ICO Children's Code, which can apply to online services likely to be accessed by children. It is not safe to assume it is irrelevant just because the service is not specifically aimed at children.

A proportionate Data Protection Impact Assessment (DPIA) and safeguards need consideration. Relevant issues include children's privacy, default settings, data collection, profiling, transparency and whether age assurance is proportionate to the risks.

Do not automatically conclude that every user under 18 needs parental consent for all data processing. The legal position depends on the processing, lawful basis, service and contractual arrangements. In particular, data-protection consent rules for children are not the same as the rules governing a child's ability to enter a paid subscription contract.

Current checklist status: The children's DPIA has been started, but the risks and safeguards are incomplete. The approach to ages 13–17, parental involvement, age assurance and paid subscriptions remains unresolved.

5. Website policies

We have worked on drafts of the following documents:

1. Privacy Policy

2. Terms of Service

3. Subscription/Cancellation Policy

4. Cookie and Browser Storage Policy

These are drafts, not a declaration that the site is compliant.

Privacy Policy

The draft covers:

• Who operates the website.

• Firebase accounts and user data.

• Collection details, duplicate records, checklist progress and scan results.

• OpenAI card scanning.

• Stripe subscriptions.

• Service providers, including Firebase/Google, Netlify, OpenAI and Stripe.

• International processing.

• Retention and account deletion.

• Children's privacy.

• User rights, security, policy changes and contact details.

The policy needs to accurately reflect actual data flows, retention, lawful bases, processors, international transfers and deletion behaviour.

Terms of Service

A draft exists but still needs finalisation. It should reflect the actual service, user responsibilities, acceptable use, availability, limitations and other applicable contractual terms without making unlawful exclusions of consumer rights.

Subscription/Cancellation Policy

A draft exists but still needs finalisation. It must accurately explain:

• The £5 monthly recurring subscription.

• When payments are taken.

• How to cancel.

• When access ends after cancellation.

• Refunds and statutory consumer rights.

• Any applicable rules concerning online digital services and cancellation rights.

• The checkout information customers receive before paying.

Do not assume that all refunds can be refused or that a generic “no refunds” clause is sufficient.

Cookie and Browser Storage Policy

A draft was prepared on 16 October 2026. It describes the site's known local/session storage and third-party services, distinguishes essential from non-essential technologies, explains browser controls and refers users to the Privacy Policy.

Do not publish it as final until the live audit is complete. If the audit finds additional cookies, tracking or other storage, update the policy and implement any required consent controls.

The UK ICO's guidance on cookies and similar technologies is an important reference. In general, users must be informed about relevant technologies and consent is required unless an exemption applies. Similar technologies can include browser storage and other methods of accessing or storing information on devices. Where consent is required, withdrawing it should be as easy as giving it.

6. Master compliance checklist

Use this as the working checklist. Items marked as unfinished must not be treated as completed merely because a draft exists.

A. Privacy and data protection

- ■ Complete the Children's Code/DPIA assessment, including risks and safeguards.
- ■ Decide the approach to users aged 13–17 and parental involvement.
- ■ Audit cookies and browser storage on the live website.
- ■ Verify Firestore scan-log expiry, TTL configuration and actual retention.
- ■ Test account deletion across Firebase Authentication, Firestore and Stripe-related records.
- ■ Verify OpenAI data-sharing settings, model eligibility and retention arrangements.
- ■ Identify and document a lawful basis for each personal-data processing purpose.
- ■ Check service providers, data-processing arrangements and international transfers.
- ■ Establish a process for privacy requests and personal-data breaches.

B. Website policies

- ■ Finalise and publish the Privacy Policy.
- ■ Finalise and publish the Terms of Service.
- ■ Finalise and publish the Subscription/Cancellation Policy.
- ■ Finish the live cookie audit, then finalise and publish the Cookie Policy.
- ■ Make policy links easy to find on the website.
- ■ Ensure users can see the relevant terms during registration and checkout where appropriate.

C. Subscriptions and consumer rights

- ■ Check recurring-payment disclosures.
- ■ Verify the cancellation process and what happens to paid access.
- ■ Check refund terms and statutory rights.
- ■ Verify all required information appears before checkout is completed.
- ■ Establish a complaints and support process.
- ■ Assess subscriptions by under-18s, including contract capacity and parental involvement.

D. Business details and younger users

- ■ Determine appropriate public business/contact details without unnecessarily exposing my home address.
- ■ Decide the minimum-age policy and any parental involvement.
- ■ Implement proportionate privacy safeguards for younger users.
- ■ Keep compliance records and review them when the site changes.

7. Current position and next steps

The most recent task was **the cookie and browser-storage audit**.

The next practical step is to verify the actual live website's cookies and browser storage, rather than relying only on the ZIP inspection. This should include the normal site, signing in, using the scanner, changing scanner preferences, visiting any payment/Stripe checkout pages, and checking what is stored before and after those actions.

After that, continue through the master checklist, with particular attention to Firestore TTL/retention and the children's DPIA.

How I want the next ChatGPT account to continue

1. Read this handover and continue from the current cookie-audit stage.
2. Ask me for only the next necessary piece of information at a time.
3. Give specific instructions for testing the live site, preferably on my Mac using the browser's developer tools.
4. Distinguish confirmed findings from assumptions and things that still need verification.
5. Use current official UK ICO, legislation and consumer-protection guidance when legal accuracy depends on it.
6. Keep the master checklist updated as we progress.
7. Do not claim the website is compliant until the relevant checks have actually been completed.
8. Keep the advice practical and proportionate for a small sole-trader website.

This is a working compliance assessment, not formal legal advice. For any high-risk or genuinely uncertain legal issue, explain what needs specialist confirmation rather than guessing.