Final Whistle Card Collection — Privacy Requests & Personal Data Breach Procedure

Status: Working operational procedure — review and adopt before launch.

Service: Final Whistle Card Collection

Contact: lennonarthurclarke09@outlook.com

Owner: Sole trader operating Final Whistle Card Collection

Last reviewed: 17 October 2026

This document is an internal operating procedure, not a substitute for legal advice. It must reflect the service's actual systems and be followed in practice.

1. Handling a privacy request

Requests can arrive by email, through the website, or through another channel. A request does not need to use legal terminology. Treat requests to access, correct, delete, restrict, object to, or obtain a copy of personal data as potential data-protection requests.

Steps

1. **Log the request promptly.** Record the date received, contact channel, request type, identity-check status, deadline, actions, and response date in a restricted-access request log. Do not put passwords, payment-card details, or unnecessary sensitive information in the log.

2. **Acknowledge receipt.** Explain that the request is being reviewed and ask for clarification only where genuinely needed.

3. **Verify identity proportionately.** Use the signed-in account or a reply from the account's verified email where appropriate. Ask for additional evidence only if there is a reasonable doubt about identity. Do not routinely demand identity documents.

4. **Clarify scope if necessary.** Identify the relevant account and data. Search the systems actually used, which may include Firebase Authentication and Firestore, Stripe for billing records, Netlify logs, and OpenAI-related operational records. Do not claim access to provider-held data that you cannot retrieve.

5. **Check exceptions and other people's rights.** For example, some billing or security records may need to be retained for legal obligations or legitimate claims. Do not delete another person's data as part of a request.

6. **Respond without undue delay and normally within one month** of receipt. If a request is complex or there are multiple requests, the legal extension rules may allow up to two further months; tell the requester within the first month and explain why. If refusing or limiting a request, explain the reason and available complaint/appeal rights.

7. **Complete and verify the action.** For deletion, distinguish deletion of the user's account from records that must lawfully be retained. Check any relevant backups/retention cycles and explain limits accurately. Do not promise immediate removal from every provider or backup unless verified.

8. **Close the log.** Record what was searched, what was supplied/changed/deleted, any reason for withholding data, the date of response, and any follow-up.

Requests involving children or a parent

Treat the child's rights and best interests as central. Verify who is making the request and their authority where a parent or guardian acts for a child; do not automatically disclose a child's information to a parent without considering the child's competence, safety, confidentiality, and applicable law. Escalate uncertain or sensitive cases for advice.

Suggested acknowledgement

Thanks for contacting Final Whistle Card Collection. I've received your privacy request and will review it. I may contact you if I need to clarify the request or reasonably verify your identity. I aim to respond without undue delay and normally within one month.

2. Personal data breach response

A personal data breach can include accidental disclosure, unauthorised access, loss, alteration, or unavailability of personal data. A suspected incident must be assessed promptly; do not wait until every detail is known.

Immediate response checklist

■ Record when the incident was discovered and who reported it.

■ Contain the incident where safe: revoke exposed credentials, disable affected access, correct a misconfiguration, or contact the relevant provider. Preserve evidence and logs; do not destroy evidence while trying to clean up.

■ Identify the systems, data types, approximate number of people affected, and whether children are affected.

■ Assess likely consequences for people, including account takeover, fraud, exposure of collection/account details, or risks to children.

■ Record the decision, reasoning, facts known, uncertainties, and containment actions, even if the incident is ultimately not reportable.

■ Contact relevant providers promptly and obtain their incident details where they are involved.

■ Decide whether the ICO must be notified. If the breach is likely to result in a risk to people's rights and freedoms, notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. If notification is later, explain the delay.

■ If the breach is likely to result in a **high risk** to individuals, communicate with affected people without undue delay unless a lawful exception applies. Use clear language and explain what happened, likely effects, steps taken, and what they can do.

■ Record any ICO notification, individual communications, and reasons for not notifying.

■ Review root cause and implement corrective actions; test the fix and update this procedure if needed.

Incident log fields

Incident reference; date/time discovered; date/time likely occurred (if known); reporter; systems/providers; categories and approximate volume of data/people; child users affected; containment steps; risk assessment; ICO decision and rationale; communications; remedial actions; owner; closure date.

3. Useful contacts and escalation

• **Service privacy contact:** lennonarthurclarke09@outlook.com

• **ICO guidance/reporting:** https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

• **ICO data protection guidance:** https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

If a serious incident involves children's data, credentials, payment access, or uncertainty about the reporting threshold, prioritise containment and seek appropriate professional advice promptly.

4. Before launch — owner sign-off

■ Choose a secure, access-restricted place for the request and incident logs.

■ Confirm who will monitor the contact email and how often.

■ Confirm how to export/search account data from Firebase and billing data from Stripe.

■ Confirm how to contact Netlify, Firebase/Google, Stripe, and OpenAI about an incident.

■ Make sure backups/log retention and account-deletion behaviour match the public privacy policy.

■ Review this procedure after a significant system change or incident, and at least annually.