

Account deletion and personal data erasure policy

Soccer Shooters | All customer systems and records

Purpose and scope

We remove personal data when it is no longer needed and respond to requests for account deletion fairly, securely and promptly. This policy covers parent and carer accounts, children's profiles, leads and customer records across all systems and records we use, including booking, customer management, payment, communication and storage systems, exports, paper records and backups.

This policy applies regardless of the software, supplier or storage method we use. It covers current systems, replacement systems, legacy systems and records transferred between them. It applies to staff, managers and suppliers handling these records. For franchise bookings, identify the legal entity responsible for the data and coordinate with that entity. Do not assume head office controls all franchise customer records.

What each request means

- Account closure disables access and ends the customer account. It does not, by itself, erase every record or cancel a payment subscription.
- Subscription cancellation stops future membership payments according to the agreed cancellation arrangements. It is separate from account deletion.
- Marketing opt out stops promotional messages. Keep only the minimum suppression information needed to prevent further marketing.
- Personal data erasure removes personal information where the right applies. Where some records must be retained, remove the rest and explain the limited retention.

Responsibilities

All staff must recognise requests, including verbal requests, and pass them to the policy owner on the day received or next working day. The policy owner decides what can be deleted, approves exceptions and oversees responses. An authorised administrator carries out the changes. A second authorised person verifies completion where practicable.

The safeguarding lead decides how safeguarding and child welfare records must be protected. Finance confirms any accounting, refund or payment records needed. Our system suppliers must support secure deletion and provide evidence of what was done.

Before this policy goes live

The owner must confirm the correct legal entity and published contact route, approve the proposed routine retention periods on page 3, and obtain supplier confirmation of deletion functions, linked record handling, integration behaviour and backup expiry periods. Staff must not describe a record as permanently deleted unless this has been verified.

Handling a deletion request

1. Record the request. Log the date received, wording, contact route, systems involved and response deadline. A customer need not use a special form or mention GDPR. Acknowledge promptly; our internal target is two working days.
2. Verify identity proportionately. Use the existing verified email or account authentication where possible. Request extra identification only where there is reasonable doubt; do not routinely collect passports. For a child's information, assess the requester's authority, the child's understanding and wishes, and any family restrictions. Do not assume that every adult linked to an account may authorise deletion of all children's data.
3. Clarify scope where needed. Establish whether the request concerns a single child, a household, account closure, marketing or all personal data. Clarification must not create unnecessary delay. Protect records belonging to other carers or children.
4. Stop unwanted marketing. Where marketing consent is withdrawn or marketing is opposed, stop promotional messages immediately and remove the contact from campaigns, scheduled sends and automations. Continue only necessary lawful service communications.
5. Check bookings and payments. Identify future bookings, active subscriptions, outstanding refunds, disputes and payments made through childcare payment services. Explain the impact of account closure and arrange cancellation or refunds as appropriate. Confirm payment cancellation with the relevant payment provider; deleting a booking or customer record alone is insufficient.
6. Decide on each data category. Identify information that can be erased and any minimum records needed for legal obligations, safeguarding or legal claims. Record the specific basis, purpose, access restrictions and review or deletion date. An unpaid balance does not justify retaining the entire profile.
7. Execute and verify. Follow the system checklist on page 4. Keep retained records in a restricted location and remove unnecessary copies. Notify recipients of erasure unless impossible or disproportionate; document any exception. On request, tell the individual who those recipients are.
8. Respond and close. Explain what was erased, what remains and why, its retention period or review criteria, and any backup limitations. Record completion evidence and the final response. Do not claim deletion across systems that have not been checked.

Deadlines and refusals

Respond without undue delay and normally within one calendar month of receipt. Set an internal completion target of 28 days. Where identity evidence is reasonably necessary, calculate the deadline in line with ICO guidance and ask for it promptly. Do not assume that other clarification pauses the deadline.

For complex requests or multiple requests from the same person, a further two months may be available. Tell the person within the first month and explain why. Supplier delays do not automatically justify an extension.

Requests are normally free. Refer any proposed refusal or fee to the policy owner. Explain any refusal or partial refusal, the reasons and the rights to complain to the ICO and seek a judicial remedy. Erasure is not an absolute right; exceptions must be specific and justified.

Retention and routine deletion

The periods below are proposed internal defaults for approval, not universal statutory requirements. An individual erasure request must be assessed when received and must not be delayed until a routine retention date. Review inactive records quarterly. A login alone does not justify indefinite retention.

Record category	Proposed rule or required action
Unused customer accounts	Review after 12 months with no booking, payment, current membership or unresolved matter. Delete unnecessary account and child profile data after review.
Unconverted enquiries and trials	Delete or anonymise after 12 months from the last substantive enquiry or trial, unless a documented ongoing purpose remains. Marketing permissions must be assessed separately.
Former customer accounts and profiles	Review 24 months after the last service or substantive contact. Delete unnecessary profiles and notes; retain only separately justified records.
Accounting and payment evidence	Keep necessary company tax records for 6 years from the end of the relevant company financial year, or longer where required. Retain minimum invoice and transaction details, not complete child profiles.
Attendance and ordinary booking history	Use a documented schedule based on setting duties, insurance and claims needs. Separate necessary evidence from redundant profiles. Confirm any applicable Ofsted requirements before deletion.
Medical and emergency contact data	Remove promptly when no longer needed for care. If relevant to an incident or claim, retain only the necessary evidence under a restricted schedule.
Accident and safeguarding records	Exclude from automatic account deletion. The safeguarding lead must confirm applicable legal, setting, insurer and child claim requirements and document retention and review dates.
Marketing suppression record	Keep minimum contact identifier, channel and objection date while needed to prevent unwanted marketing. Restrict use to suppression and review necessity periodically.
Deletion request audit log	Proposed 3 years after completion, subject to documented necessity. Keep a reference, decision, dates, retention exceptions and verification evidence; avoid copies of whole profiles or identity documents.

Retention exceptions

A documented investigation, complaint, claim or legal hold suspends deletion of relevant evidence only. Review the hold regularly and delete when it ends and no other purpose remains. Retained data must not remain available for marketing or ordinary coach access. Anonymisation must prevent identification; replacing a name with an account number is not anonymisation.

System deletion checklist

- Booking and account systems: locate parent accounts, linked children, duplicate accounts, contact and emergency details, medical notes, bookings, registers, uploaded files and consent records. Confirm effects on other household members before deletion.
- Payment systems: check all connected payment providers, including any childcare payment services. Confirm subscription cancellation and necessary refund handling separately. Preserve legally required transaction evidence with restricted access; assess deletion of redundant customer profiles. Record any provider retention obligations.
- Customer management and communication systems: locate duplicates, contacts, child details, notes, messages, attachments, forms, pipelines, tags, smart lists, tasks, campaigns and scheduled automations. Remove unnecessary data and apply marketing suppression in every sending channel.
- Integrations: prevent synchronisation, webhooks, imports or retry queues from recreating deleted records. Apply deletion across connected systems and verify after the next normal sync cycle. A future genuine booking is a new relationship and must not automatically restore marketing consent.
- Other copies: check staff exports, spreadsheets, email attachments, shared drives, archived marketing tools and printed registers. Securely delete unnecessary copies. Do not circulate personal data in deletion confirmation tickets.
- Verification: search by the authorised identifiers in each system, check the relevant record relationships and obtain supplier confirmation where deletion is not directly visible. Keep reference numbers and dates rather than screenshots containing excess personal data.

Backups and technical limitations

Ask each supplier to confirm its backup retention and deletion arrangements in writing. Where immediate removal from backups is not feasible, put the information beyond use until backups expire under the documented schedule. It must not be used for ordinary processing. Record the expected expiry date and explain this to the individual.

After restoration, reapply deletion and suppression controls before the restored system returns to ordinary use. If a system offers only archive or deactivate functions, do not treat these as erasure. Restrict access and use, escalate to the supplier, and provide an accurate response within the deadline.

Deletion log fields

Request reference; date received; scope; identity and authority check outcome; responsible legal entity; deadline; staff owner; systems and supplier ticket references; decision and lawful retention reasons; retained categories and expiry or review dates; actions and verification dates; recipients notified; backup expiry; response date; closure date.

Reference guidance

Checked 5 October 2026. ICO guidance is being updated following the Data Use and Access Act; check current guidance when handling unusual requests.

ICO Right to erasure: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/>

ICO Right to object: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-object/>

GOV UK Company and accounting records: <https://www.gov.uk/running-a-limited-company/company-and-accounting-records>