Advance Gymnastics Club

Internal Data Protection Policy

Version 1.1 — Last updated: 27 July 2026

1. Purpose

This policy sets out how Advance Gymnastics Club complies with the UK GDPR and Data Protection Act 2018 when running its website, member app and in-person classes.

This is the club's INTERNAL data protection policy — the working document for the owner, admin users and coaches. It sits alongside (not instead of) the public Privacy Policy, and is what the ICO would ask to see first in any complaint or investigation. It is not intended for publication in its current form.

2. Roles & Responsibilities

- Data Controller: Club owner — Megan.
- Day-to-day Data Protection Lead: Megan.
- Welfare / Safeguarding Officer: Deb — advancegymwelfare@gmail.com.
- Data Protection Officer (DPO): The club is not legally required to appoint a DPO under UK GDPR Art. 37 as it does not carry out large-scale monitoring or process special category data at scale. The Data Protection Lead (Megan) fulfils equivalent duties and is the point of contact for all data protection matters.
- Processors: Supabase / Lovable Cloud, Stripe, Cloudflare, and the club's email provider — each engaged under a written contract / DPA.

3. Lawful bases we rely on

Contract, Consent (for marketing, photography/video and health data), Legitimate Interests (for security and safeguarding-adjacent activities), Legal Obligation (tax, safeguarding reporting). A separate Record of Processing Activities (ROPA) documents this per activity.

- Purchase and booking records are kept under legal obligation (HMRC / accounting law) and contract.

4. Data Minimisation & Accuracy

We will:

- Only collect the fields listed in the sign-up form and booking form.
- Review the sign-up form yearly and remove fields no longer used.
- A parent's account may store details for one or more children.
- After approval, changes to a child's details are made by the club administrator on the member's request via info@advancegymnasticsclub.com.

- Coaches see only the name / class of children in their classes, not full contact details.

5. Security Controls

- Passwords must contain at least 8 characters including uppercase, lowercase, a number and a special character, and are additionally checked against a public database of known breached passwords.
- Passwords are hashed by Supabase Auth. They are never emailed and never stored in plain text.
- Row-Level Security (RLS) is enabled on every database table containing personal data.
- Admin actions are logged (audit trail visible in the Analytics tab).
- Multi-factor authentication (email OTP) is required for new devices, with a 60-day trusted-device window.
- Only the club owner (and any explicitly-appointed deputy) has admin access.
- Devices used to access the admin dashboard must have a screen lock and up-to-date OS.
- Public Wi-Fi must not be used for admin work without a VPN.
- Any lost or stolen device with admin access must trigger an immediate password reset.

6. Special Category Data

Certain information the club may receive is treated as "special category" data under UK GDPR Article 9 and requires additional safeguards. This includes:

- Health, medical or disability information relevant to safe participation.
- Injury records and any safeguarding disclosures.

Where such data is collected:

- It is collected only with explicit consent from the parent / guardian (or adult member), or where necessary for safeguarding or vital interests.
- It is stored in restricted-access records, visible only to the club owner and, where directly relevant to safe supervision, the assigned coach.
- It is never used for marketing or shared beyond the club except where required by law or safeguarding duty.
- It is deleted or anonymised as soon as it is no longer required for the purpose collected.

7. Photography & Video Consent

- Photographs and video containing identifiable members (especially children) are only taken or used with explicit written consent from the parent / guardian, obtained via the consent form.

- Consent is recorded per member and can be withdrawn at any time by contacting info@advancegymnasticsclub.com.
- Withdrawal takes effect promptly and, at the latest, within 30 days for existing published material where it is within the club's control to remove.
- Images and video are stored securely and are not shared with third parties for commercial use.
- Coaches, members and parents may not publish images of other children on personal social media without the club's written approval.

8. International Data Transfers

Some of the club's processors (for example Stripe, Cloudflare and email providers) may process personal data outside the UK, typically in the EEA or the USA. Where this happens:

- The club relies on UK-approved safeguards such as the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or an adequacy decision (e.g. the UK–US Data Bridge).
- Copies of the relevant DPAs and transfer mechanisms are downloaded from each processor and kept on file.
- The processor list is reviewed at least annually to confirm the transfer basis is still valid.

9. Data breach procedure

- Any suspected breach is reported immediately to the club owner.
- Assess within 24 hours whether it is likely to result in a risk to the rights and freedoms of individuals.
- If yes, notify the ICO within 72 hours of becoming aware, via ico.org.uk.
- If high risk (e.g. exposure of children's data), notify affected members without undue delay.
- Log every breach — including near misses — in the internal breach register.

10. Subject rights procedure

All Subject Access Requests (SARs), erasure and rectification requests are handled by the club owner within one month of receipt. Identity must be verified before releasing data. A log of all requests is kept.

Financial records cannot be deleted on request while the statutory retention obligation applies.

11. Children's data & safeguarding

The club does not create accounts for children under 18. All accounts, bookings and communications relating to under-18s are held under the parent or guardian's account.

- Data on under-18s is provided by parents / guardians.
- Class assignments and welfare notes are visible only to the club owner and the assigned coach.
- Safeguarding disclosures follow the club's Safeguarding Policy and are shared with statutory authorities where required.
- Requests should be made via: info@advancegymnasticsclub.com

12. Processors & third-party checks

- A Data Processing Agreement (DPA) is signed with each processor before use. Most (Stripe, Supabase, Cloudflare) publish standard DPAs online — these are downloaded and filed.
- Processors are reviewed annually. Access is removed when a processor is no longer used.
- The list of processors in the public Privacy Policy is kept up to date.

13. Marketing & consent

- Marketing consent is never bundled into the sign-up form as a pre-ticked box.
- Evidence of when and how each member opted in is retained.
- Every marketing email includes a working unsubscribe link.
- Unsubscribes are actioned within 5 working days.

14. Training & Culture

Anyone with admin or coach access reads this policy and the Safeguarding Policy on appointment and re-reads them annually. The date of each read / refresher is recorded in a simple training log.

15. Retention & deletion

Follow the retention schedule published in the Privacy Policy. A review is run every 12 months to delete data past its retention period.

- Active members — during membership.
- Former members — up to 1 year for safeguarding reasons.
- Accident records — as required by law.
- Financial transaction records — 6 years (HMRC requirement).

Deletion means removal from live systems and from backups within the backup rotation window.

- Backups are managed by the hosting provider (Supabase). Encrypted backups are retained for up to 30 days on a rolling window, after which they are overwritten. Deletion requests are honoured in the live system immediately and will fall out of backups within this 30-day window.
- The backup restore procedure is documented separately.

16. Website & app-specific controls

- Only 'strictly necessary' cookies / local storage are used. Any change (e.g. adding analytics) requires a consent banner to be added first.
- Payment card data never touches the club's servers — Stripe handles it via their hosted checkout.
- Policy documents that contain member-only content are gated behind sign-in via the PolicyLink component.
- The admin approval workflow ensures no unverified account can see member-only data.
- The Analytics / Audit log records every admin action against member data.

17. Refunds

- Refund handling — full refunds are processed via Stripe by admin request and typically appear within 5–10 working days.
- Purchase and booking history is retained in the club's accounting records.
- Member credits are automatically released when a refunded booking used one.

18. Version control & review

This policy is reviewed at least annually, or whenever a significant new feature (e.g. mobile app launch, new payment method, marketing analytics) is added. The version number and review date appear at the top of this document.