

Privacy Policy

How The Sporting Network collects, uses, and protects your personal data.

VERSION	2.6
EFFECTIVE FROM	18 September 2026
LAST UPDATED	18 September 2026
PUBLISHED AT	thesportingnetwork.com/privacy
CONTROLLER	The Sporting Network Limited · Company no. 16989082 · ICO ZC110454

1.1

About This Policy

This Privacy Policy explains how The Sporting Network LTD ("we", "our", "us", or "the Company") collects, uses, stores, shares, and protects personal data when you access or use our platform at thesportingnetwork.com (the "Platform") and any associated mobile applications, APIs, or services.

The Sporting Network is a networking and talent-discovery platform for sport, enabling athletes, coaches, clubs, scouts and institutions to build profiles, discover one another, communicate, and manage teams.

This Policy is issued in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR), and any successor legislation. Where we process data of individuals in the European Economic Area, we also comply with the EU General Data Protection Regulation (EU GDPR).

By creating an account or using our services, you acknowledge that you have read, understood, and agree to the practices described in this Privacy Policy. If you do not agree, you must not use the Platform.

1.2

Data Controller

- **Data Controller:** The Sporting Network LTD
- **Registered Address:** 14 Hollywell Row, London, England, EC2A 4JB
- **Company Registration:** 16989082
- **ICO Registration:** ZC110454
- **Data Protection Contact:** main@thesportingnetwork.com
- **Data Protection Officer:** Not currently required. We have assessed this and keep the position under review.

Age Eligibility and Protections for Users Under 18

The Platform is intended only for individuals aged 13 years or older. We do not knowingly collect or process personal data from individuals under the age of 13, and accounts cannot be created without passing our date-of-birth age gate. If we become aware that we have inadvertently collected personal data from a person under 13, we will take prompt steps to delete the account and all associated personal data. If you believe a child under 13 has created an account, please contact us immediately at main@thesportingnetwork.com.

Users aged 13–17 receive the following additional protections:

- **Accounts are private by default.** An account held by a user aged 13–17 is private from the moment it is created. It becomes visible to the wider Platform only if the young person chooses to make it public, and they can make it private again at any time. Accounts held by users aged 18 and over are public by default.
- **A private account is fully private.** A private account is not visible to anyone who is not a connection — it does not appear in search or discovery of any kind, including scout search, and it cannot be viewed directly by following a link. This restriction cannot be bypassed by any account type, including verified coach, scout, and team accounts.
- **Field-level privacy controls.** Whether your account is public or private, you may set individual profile fields to public or private. Fields you mark private are not visible to anyone who is not a connection, and this restriction likewise cannot be bypassed by any account type.
- **No shareable profile links.** Accounts held by users under 18 cannot generate or share a profile link, whether or not the account is set to public. An under-18 profile therefore exists only within the Platform and cannot be circulated outside it.
- **Contact is gated.** Any message from a user you are not connected with goes to a request inbox. It does not reach your main conversations unless and until you accept it.
- **Search and contact require verified identity.** An account registered as a coach, scout, club, academy or team must complete identity verification through Persona before it can start a new conversation with any user, or use scout search — the filtered search of athletes, including by location.
- **No analytics and no advertising identifiers.** We do not collect analytics data or advertising identifiers on accounts held by users under 18. Analytics collection is disabled entirely for these accounts, not merely limited. The record of what you engage with that we use to order your own feed (see the next point) is not analytics and is used for nothing else.
- **Nothing you post is sent to our AI providers for feed ranking.** We use OpenAI to analyse the text of public posts, and Anthropic to describe the photos and video stills in them, so that we can order feeds (see section 1.7(c)). Nothing written or uploaded by a user under 18 is sent for this purpose, whether it is a personal post or a team post. This exclusion is built into the Platform and cannot be switched off, and where we do not hold a confirmed date of birth we treat the account as under 18 for this purpose.
- **Your feed is not personalised unless you choose it.** For users under 18, personalised ordering is off by default. We do not record which posts you are shown or how you interact with them, and we do not build a feed preference profile. You may switch personalisation on in Settings → Privacy → Discover feed; if you do, the same 90-day deletion and safeguards described in section 1.7(c) apply, and switching it off again deletes the record and the profile immediately.

- **identity verification is optional.** Users under 18 may choose to complete identity verification, but it is never required in order to create an account, build a profile, or use the Platform.

We encourage parents and guardians of users under 18 to be aware of their child's use of the Platform, and welcome contact at the address above with any questions or concerns. A short guide written for users under 18, *Your Privacy, Explained*, is also available on the Platform.

1.4

Information We Collect

(a) Information You Provide Directly

When you register for an account, create a profile, or use Platform features, you may provide us with the following categories of personal data:

- Full name, display name, or username
- Email address
- Password (stored in hashed form only)
- Date of birth (used to verify age eligibility and apply age-appropriate protections; not displayed publicly)
- Profile information such as biography, sport(s), position, team affiliation, and optional location
- Profile photographs and uploaded media (images and video)
- Athletic statistics, performance data, and sporting achievements
- **Health and fitness information**, where you choose to provide it. This includes injury history, VO₂ max, body fat percentage, resting and maximum heart rate, and sleep hours. This is special category data concerning health under Article 9 of the UK GDPR. Every field is optional, and we collect this information only where you have given your separate explicit consent at the point of entry (see section 1.5). You may withdraw that consent and delete this information at any time.
- Academic grades, where you choose to provide them, used for the university eligibility filter
- Identity verification data where you verify your account: images of a government-issued identity document and a live selfie, processed by our identity verification provider (see sections 1.10 and 1.16)
- Messages sent through the Platform's messaging features
- Comments, posts, and other user-generated content
- Conversations with our AI assistant, including the messages you send and profile information shared with the assistant to answer your questions (see sections 1.6 and 1.10)
- Reports, feedback, or communications sent to our support team
- Any other information you choose to provide

(b) Information Collected Automatically

When you access or use the Platform, we automatically collect certain technical and usage data, including:

- IP address and approximate geolocation derived from IP
- Device type, operating system, and version

- Browser type and version
- Unique device identifiers
- Mobile advertising identifiers (e.g. the Android Advertising ID), used for analytics and measuring the performance of our advertising campaigns. These are collected only on accounts held by users aged 18 and over. No advertising identifier is collected before a date of birth has been provided and confirmed as 18 or over.
- Push notification tokens for your device, where you have enabled notifications
- Precise device location (GPS), only where you grant the app location permission, used to show nearby events and to help you set event locations; you can decline or revoke this permission at any time in your device settings
- Log data including pages visited, features used, timestamps, and referring URLs
- Session duration and interaction data
- **Feed engagement data:** a record, held on our own servers, of the posts shown in your feed and how you interact with them, used only to order your feed. Each entry is deleted automatically after 90 days (see section 1.7(c)). It is kept only where personalised ordering is on: by default for users aged 18 and over, and only by choice for users under 18 (see section 1.3).
- Security and authentication data (e.g. login attempts, failed authentication)
- Cookie data and similar tracking technologies (see our Cookie Policy)

(c) Information We Derive

- **Feed preference profile:** a set of 512 numbers that summarises the kinds of posts you engage with, used only to order your own feed. No other user can access it. For users under 18 it is not built unless they switch personalised ordering on (see section 1.7(c)).
- **Post embeddings:** numerical representations of the text of public posts, used to measure how similar posts are to one another (see section 1.7(c)).
- **Post media descriptions:** a short written description of the sport, activity and setting shown in a photo or video still from a public post, produced by our AI provider and stored with the post (see section 1.7(c)). It never names or describes a person.

(d) Information from Third Parties

We may receive personal data about you from third-party sources in limited circumstances, including:

- Authentication providers if you use single sign-on, including Sign in with Google and Sign in with Apple
- Our identity verification provider, Persona, which confirms the outcome of an identity verification you initiate
- Publicly available information to verify identity or prevent fraud
- Law enforcement or regulatory bodies in connection with investigations

1.5

Legal Bases for Processing

We process personal data only where we have a lawful basis to do so under the UK GDPR:

- **Contract (Article 6(1)(b)):** Processing necessary to perform our contract with you, including providing your account, delivering Platform features, enabling messaging and networking, providing the AI assistant where you choose to use it, and translating content you have asked to have translated.
- **Legitimate Interests (Article 6(1)(f)):** Processing necessary for our legitimate interests or those of a third party, provided those interests are not overridden by your rights. This includes security monitoring, fraud prevention, platform improvement, analytics, **the automated checks applied to messages described in section 1.7, ranking the posts in your feed as described in section 1.7(c)**, the automatic hiding of content reported by multiple users, the initial triage of reported content, and enforcing our Terms.
- **Consent (Article 6(1)(a)):** Where we rely on your consent, such as for non-essential cookies, marketing communications, or future advertising features. You may withdraw consent at any time.
- **Legal Obligation (Article 6(1)(c)):** Processing necessary to comply with a legal obligation, such as responding to court orders, regulatory requirements, or law enforcement requests, and complying with our duties under the Online Safety Act 2023.
- **Vital Interests (Article 6(1)(d)):** In exceptional cases, processing necessary to protect the vital interests of an individual, such as safeguarding concerns involving minors.

Special Category Data (Article 9)

Some of the data we process is special category data, which receives additional protection under Article 9 of the UK GDPR. We process it only where one of the following conditions applies:

- **Explicit Consent — Health and Fitness Data (Article 9(2)(a)):** Where you choose to provide health and fitness information, including injury history and physiological metrics, we ask for your separate explicit consent at the point you enter it. This consent is specific to health data, is not bundled with our Terms or any other agreement, and is recorded with the date and the version of this Policy in force. Providing this information is entirely optional, the Platform is fully usable without it, and you may withdraw your consent and delete the information at any time through your profile settings.
- **Explicit Consent — Biometric Data (Article 9(2)(a)):** Where you verify your identity, our verification provider processes biometric data (a facial scan derived from your selfie and identity document) for the purpose of uniquely confirming that you are the document holder. This processing takes place only with your explicit consent, which you may decline. Where explicit consent cannot be relied upon, we rely instead on the safeguarding condition immediately below. Verification is not required to create an account or to use the Platform generally, but it is required before a coach or scout can start a new conversation or use scout search (see section 1.16).
- **Safeguarding (Article 9(2)(g), and Schedule 1 Part 2 paragraph 18 of the Data Protection Act 2018):** Where we process special category data as necessary for the protection of children or of individuals at risk of harm, including in the course of investigating a safety report and where we rely on this condition for identity verification. This is a substantial public interest condition recognised in UK law. Where we rely on it we maintain an Appropriate Policy Document, which is held internally and produced to the Information Commissioner on request.
- **Legal Claims (Article 9(2)(f)):** Where processing is necessary for the establishment, exercise, or defence of legal claims.

We do not use health or fitness data for advertising, and we do not disclose it to third parties for their own purposes. Where you have marked health fields private, they are not visible to anyone who is not a connection, and that restriction cannot be bypassed by any account type.

How We Use Your Information

Service Delivery

- Creating, maintaining, and administering user accounts
- Providing core Platform functionality including profiles, networking, and content sharing
- Ordering the posts in your feed so that those most relevant to you appear first (see section 1.7(c))
- Enabling private and group messaging features, including the request inbox
- Delivering push notifications you have enabled
- Verifying the identity of users, including where verification is required to start a conversation or to access scout search
- Displaying user-generated content as intended

AI-Assisted Features

We use Anthropic's Claude models to provide four features. In each case the data is processed on our instructions under a data processing agreement, and is not used to train any model:

- **AI assistant.** Where you choose to use the in-app assistant, your conversation and relevant profile information are sent to Anthropic so that the assistant can answer your question. Where your profile contains health and fitness data and that data is relevant to your question, it may form part of what is sent. The assistant is available to all users, including users under 18.
- **Content moderation triage.** Where content is reported to us, it is sent for automatic classification to help us prioritise review. What is sent includes the reported content and the conversation or thread in which it appears, the display name and username of the account concerned, and whether that account is held by a user under 18. This classification is advisory only and never determines an outcome on its own (see section 1.15).
- **Translation.** Posts, comments, and profile biographies are translated where a user requests a translation.
- **Feed ranking (media).** Where you have agreed to it, each photo in a public post you make, or a single still frame from each video, is sent to Anthropic, which returns a short description of the sport, activity and setting shown, for example "a golfer driving from a tee on an outdoor course". Anthropic is instructed not to identify or describe any person, and derives no facial or biometric data. We keep the description with the post and include it in the text sent to OpenAI (below).

We also use OpenAI's embedding models for one feature, **feed ranking**: the text of public posts, together with any media description produced by Anthropic, is converted into numbers so that we can measure how similar posts are. OpenAI processes this data on our instructions under a data processing agreement and does not use it to train its models. What is and is not sent is set out in section 1.7(c).

The automated checks applied to messages, described at section 1.7, are not carried out by our AI providers. They run on our own servers and no message content is sent to a third party as part of them.

Security and Safety

- Detecting, preventing, and responding to fraud, security incidents, and abuse
- Monitoring for violations of our Terms and Conditions and Community Guidelines

- Verifying user identity where necessary
- Protecting the safety of our users, particularly users aged 13–17

Platform Improvement

- Analysing usage patterns to improve features and user experience, on accounts held by users aged 18 and over
- Measuring the effectiveness of our advertising campaigns (e.g. app install and conversion measurement) using aggregated analytics and, for users aged 18 and over only, mobile advertising identifiers
- Conducting internal research and development
- Troubleshooting technical issues

Communications

- Sending service-related notifications (e.g. account verification, security alerts, policy changes)
- Responding to support requests and enquiries
- Sending marketing communications where consent has been obtained (with opt-out)

Legal and Regulatory

- Complying with applicable laws, regulations, and legal processes
- Establishing, exercising, or defending legal claims
- Responding to law enforcement requests

We do not sell, rent, or trade your personal data to any third party for their own marketing or commercial purposes.

1.7

| Messaging, User Content, and Your Feed

Private messages and user-generated content are stored on our servers to provide Platform functionality. Content you post publicly on the Platform may be viewed by other registered users.

(a) Automated checks on messages

All messages sent on the Platform pass through automated checks before they are delivered. These checks run on our own servers rather than in the app, so they apply to every message and cannot be avoided by modifying or replacing the software used to access the Platform. They:

- screen the content of messages against a list of prohibited terms; and
- screen the introductory message attached to a contact request for links, social media handles and telephone numbers, because persuading a young person to continue a conversation off the Platform is a recognised safeguarding risk.

Where a message is caught by these checks, it may be blocked or flagged for review. **These checks are automated — a computer applying a rule to text — and no person reads your messages as part of this process.** No message content is sent to any third party as part of these checks, and they do not produce a legal or similarly significant effect (see section 1.15). Our lawful basis is our legitimate interest in the safety and security of the Platform and, in particular, the protection of users aged 13–17.

if you believe a message of yours has been blocked in error, contact us at main@thesportingnetwork.com.

(b) When a person reads message content

We do not routinely monitor or read the content of private communications. A member of our team will access, review, and if necessary disclose message content only in the following circumstances:

- When a message, post, or user is reported through our reporting tools
- Where a message has been flagged by the automated checks described above and a human decision is needed
- Where we have reason to believe there is a risk of harm to a user under 18, in which case we may proactively review interactions involving that user
- When required or compelled by law, court order, or regulatory authority
- When necessary to protect the safety of users or the public, including safeguarding concerns
- When necessary to investigate a breach of our Terms and Conditions, Community Guidelines, or applicable law
- To prevent or address fraud, security threats, or technical issues

Where a message, post, or user is reported to us, the reported content and the conversation in which it appears are sent to our AI provider for triage classification, as described in section 1.6. Because a reported message forms part of a conversation, this may include messages sent by other participants in that conversation who have not themselves been reported.

(c) How your feed is ordered

The order in which posts appear in your feed is decided automatically, using four things.

- **Post embeddings.** For public posts only, we send OpenAI the text of the post, its hashtags, the author's primary sport and profile type (for example, athlete or coach), and, where the author has agreed to media analysis, the written description of the post's photos or video still produced by Anthropic. For public team posts we send the text of the post, the team's name and sport, and the same description where the person who posted has agreed. A post is public for this purpose where it is visible in the feed and its author has set post visibility to everyone. OpenAI returns an embedding, a list of numbers that lets us measure how similar two posts are, which we store on our own servers for as long as the post exists. No post written or uploaded by a user under 18 is sent to either provider, personal or team; the exclusion is built into the Platform and cannot be switched off, and an account for which we do not hold a confirmed date of birth is treated as under 18.
- **Media descriptions.** Before your first public post containing a photo or video, we ask whether you agree to its media being described for feed ranking. If you decline, or later switch it off in Settings → Privacy → Discover feed, no photo or video still from your posts is sent, any descriptions we hold are deleted at once, and your posts are re-embedded from their text alone. Descriptions are produced from the image only; captions, comments and profile information are not sent alongside it. Your posts appear in feeds as normal either way.
- **Your engagement record.** On our own servers, we record the posts shown in your feed and how you interact with them. Each entry is deleted automatically 90 days after it is recorded.

- **Your feed preference profile.** From your engagement record we calculate a set of 512 numbers summarising the kinds of posts you engage with. It is stored on our servers, database access rules prevent any other user from reading it, and it is used only to order your own feed. For users under 18 it is not built unless they switch personalised ordering on (see section 1.3).
- **Platform-wide weights.** Each night we recalculate six weights that balance the factors used in ranking. They apply to every user alike and do not relate to any individual.

What is never sent to either provider: profile biographies, messages, comments, posts visible only to connections or set to private, anything written or uploaded by a user under 18, your engagement record, your feed preference profile, or any information about who is viewing a feed. Photos and videos are never sent unless you have agreed to it, and are never sent to OpenAI.

Your engagement record and feed preference profile are never used for advertising and are never shared with any third party. The engagement record is kept only where personalisation is on: by default for users aged 18 and over, and only by choice for users under 18 (see section 1.3). Ordering your feed in this way is profiling within the meaning of the UK GDPR, but it only decides the order in which posts are shown to you and has no legal or similarly significant effect (see section 1.15). Our lawful basis is our legitimate interest in showing each user the content most relevant to them. You have the right to object to this processing (see section 1.12).

1.8

User Safety, Reporting, and Safeguarding

We take user safety seriously. Any user may report content or behaviour that they believe violates our Community Guidelines or applicable law, including but not limited to harassment, hate speech, illegal material, impersonation, grooming behaviour, or threats of violence.

Our Content Reporting and Removal Policy sets out how to make a report, the timescales we work to, the outcomes available to us, and how to appeal a decision.

When a report is received it is classified automatically to help us prioritise urgent cases. That classification is advisory: every report is reviewed by a member of our team.

One automated control acts on content before a person has reviewed it. Where three separate users report the same post, that post is hidden from view immediately. This control can only hide a post — it can never delete content, warn a user, or ban an account — the author cannot restore it themselves, and a director then reviews it and either restores it or decides on a further outcome. Aside from that, no enforcement decision is made by automated means alone. This is described further at section 5.4 of our Content Reporting and Removal Policy.

Following investigation, we may remove content, issue warnings, suspend accounts temporarily, ban accounts permanently, delete an account, or report matters to relevant law enforcement authorities or safeguarding bodies.

Where we identify a risk of harm to a child or vulnerable person, we will take immediate action, which may include contacting the relevant authorities without prior notice to the user concerned.

1.9

Data Retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law:

- **Active accounts:** Personal data is retained for the duration of your active account.
- **Deleted accounts:** Upon account deletion, we will delete or anonymise your personal data within 30 days, except where retention is required for legal, security, safeguarding, or regulatory purposes.
- **Health and fitness data:** Retained until you delete it or withdraw your consent, or until your account is deleted, whichever is earlier.
- **Identity verification data:** Your identity document images, selfie, and derived biometric data are stored by our verification provider, Persona — never by us — and are retained by Persona only as long as necessary for verification, fraud prevention, and legal compliance, after which they are deleted. We retain the verification outcome and the date it was recorded, linked to your account, for as long as the account exists and for six years afterwards.
- **Reports and moderation records:** Records of reports, decisions, and appeals are retained for as long as necessary for safeguarding, legal, and regulatory purposes, as set out in our Content Reporting and Removal Policy. These records are retained independently of the accounts involved, and are not deleted when a reported or reporting account is deleted.
- **Feed engagement record:** Each entry is deleted automatically 90 days after it is recorded and is kept only where personalised ordering is on. The whole record is deleted immediately when you switch personalisation off or when your account is deleted.
- **Feed preference profile:** Retained while your account exists and recalculated as you use the Platform; deleted immediately when you switch personalisation off or when your account is deleted.
- **Post embeddings:** Retained on our servers for as long as the post they relate to exists. When a post is deleted its embedding is deleted with it, within the 30-day window in which a deletion can be recovered. Media descriptions are retained for the same period, and are deleted immediately if you withdraw your agreement to media analysis.
- **Data processed by our AI providers:** Content sent to Anthropic for the AI assistant, translation, or moderation triage is retained by Anthropic for up to 30 days and then deleted. Where Anthropic's own safety systems flag content, Anthropic may retain that content for up to 2 years. Post content sent to OpenAI for feed ranking is retained by OpenAI for up to 30 days for abuse monitoring and then deleted. Photos and video stills sent to Anthropic for feed ranking are retained by Anthropic for up to 30 days for abuse monitoring and then deleted, on the same terms as the AI assistant. Neither provider uses any of it to train its models, and each must delete all of it within 30 days of our agreement with them ending.
- **Security and fraud logs:** Retained for up to 12 months following the relevant event.
- **Error and crash reports:** Retained by Sentry for 90 days and then deleted.
- **Legal hold:** Where data is subject to a legal hold, litigation, safeguarding investigation, or regulatory investigation, it will be retained until the matter is resolved.
- **Backups:** Data in encrypted backups may persist for up to 30 days after deletion before being overwritten.

You may delete your account at any time directly in the app (Settings → Your Data → Delete account) or on the web Platform, or by contacting us at main@thesportingnetwork.com. Deletion removes your profile, posts, and personal data in accordance with the timescales above.

1.10

Data Sharing and Third Parties

(a) Processors Acting on Our Instructions

The following providers process personal data on our behalf, under our instructions, and are bound by data processing agreements requiring appropriate technical and organisational safeguards:

- **Cloud hosting and infrastructure:** Vercel (web application hosting) and Supabase (database and authentication backend)
- **Content delivery and storage:** Supabase Storage (file and media storage)
- **Email and communication services:** Resend
- **Analytics:** Google Firebase Analytics (mobile apps), on accounts held by users aged 18 and over only
- **Advertising measurement:** Google — the Google Ads tag on the website, for measuring conversions from our own advertising campaigns, with user consent. On mobile, Google Firebase Analytics performs campaign measurement using advertising identifiers for users aged 18 and over only.
- **Identity verification:** Persona Identities, Inc. ("Persona"), which processes and stores identity documents and selfie images (including biometric facial comparison data) on our behalf when you verify your account
- **AI-assisted features:** Anthropic Ireland, Limited ("Anthropic"), which processes AI assistant conversations, reported content submitted for triage classification, content submitted for translation, and photos and video stills from public posts submitted for description in feed ranking, where the author has agreed. Processing takes place in the United States, on infrastructure operated by Anthropic PBC and its cloud sub-processors. Anthropic does not use data sent through this service to train its models.
- **Feed ranking:** OpenAI OpCo, LLC ("OpenAI"), which converts the text of public posts, with their hashtags, the author's primary sport and profile type, and for team posts the team's name and sport, into embeddings, together with the written media description produced by Anthropic where the author has agreed. It never receives photos or videos. It receives nothing written by users under 18 and no information about who views a feed. Processing takes place in the United States. OpenAI does not use data sent through this service to train its models.
- **Error and crash reporting:** Functional Software, Inc. ("Sentry"), which receives a technical report when the app or the website hits an error: the error message and the place in our code where it happened, the app version, the device model and operating system version, and a random installation identifier. Reports never contain your name, email address, messages or profile content, and Sentry discards IP addresses on receipt. Reports are sent only from accounts held by users aged 18 and over; nothing is sent from an account held by a user under 18 or for which we do not hold a date of birth. Processing takes place in the European Union. Sentry does not use data sent through this service for any purpose of its own.
- **Push notifications:** Expo (notification delivery service), Google Firebase Cloud Messaging (Android), and Apple Push Notification service (iOS)
- **Payment processing:** Not applicable at launch

Some of these providers engage sub-processors in order to deliver their services. Each is required by contract to impose equivalent data protection obligations on any sub-processor it engages, and to give us advance notice of any change so that we may object.

(b) Independent Controllers

The following organisations receive limited personal data in their own right rather than on our instructions. They determine their own purposes for that data and are governed by their own privacy policies, not by a data processing agreement with us:

- **OpenStreetMap Foundation:** Receives your IP address and the text of your search when you use location search in our mobile apps (via the Nominatim service), and when map tiles are loaded on our website.
- **Apple:** Receives map interaction data when maps are displayed in our iOS app (Apple MapKit), and account identifiers where you choose to use Sign in with Apple.
- **Google:** Receives map interaction data when maps are displayed in our Android app (Google Maps Platform), and account identifiers where you choose to use Sign in with Google.

(c) Other Disclosures

We may also disclose personal data to comply with a legal obligation, to protect the rights, property, or safety of The Sporting Network LTD, our users, or the public, in connection with a merger or acquisition, or to law enforcement or safeguarding bodies where there is a risk of harm.

1.11

International Data Transfers

As the Platform operates globally, personal data may be transferred to and processed in countries outside the United Kingdom or the European Economic Area (EEA). In particular, Persona, Anthropic and OpenAI process data in the United States.

Where such transfers occur, we ensure that appropriate safeguards are in place as required by the UK GDPR, including transfers benefiting from an adequacy decision, Standard Contractual Clauses (SCCs), the International Data Transfer Agreement (IDTA) or UK Addendum, and any other appropriate safeguard recognised under applicable data protection law.

For transfers to Anthropic, we rely on the European Commission's Standard Contractual Clauses (Module Two, controller to processor) together with the UK International Data Transfer Addendum, version B.1.0. For transfers to OpenAI, we rely on the Standard Contractual Clauses (Module Two, controller to processor) as amended by the UK International Data Transfer Addendum, incorporated in OpenAI's data processing addendum. We do not rely on the EU-US Data Privacy Framework for these transfers.

You may request further information about the safeguards we apply by contacting us at main@thesportingnetwork.com.

1.12

Your Rights

Under the UK GDPR and applicable data protection legislation, you have the following rights:

- **Right of Access (Article 15):** Request a copy of the personal data we hold about you.
- **Right to Rectification (Article 16):** Request correction of inaccurate or incomplete personal data.
- **Right to Erasure (Article 17):** Request deletion of your personal data in certain circumstances.
- **Right to Restriction (Article 18):** Request restriction of processing in certain circumstances.

- **Right to Data Portability (Article 20):** Receive your personal data in a structured, commonly used, and machine-readable format. On request we will provide your data as a structured JSON file, covering your profile, posts, comments, messages, team memberships, and any health and fitness data and consent records held.
- **Right to Object (Article 21):** Object to processing based on legitimate interests, including the use of your engagement record and feed preference profile to order your feed, or for direct marketing purposes.
- **Right to Withdraw Consent:** Where processing is based on consent, you may withdraw your consent at any time. Withdrawing consent for health and fitness data can be done directly in your profile settings and deletes the data. Agreement to feed-ranking analysis of your posts, and separately of the media in them, can be withdrawn at any time in Settings → Privacy → Discover feed, and withdrawing deletes the related embeddings and descriptions.
- **Right to Complain to Us:** You may complain to us directly about how we have processed your personal data, by emailing main@thesportingnetwork.com marking your message "Data Complaint". We will acknowledge and respond as soon as we can, and our Complaints Procedure sets out how we handle complaints, how we keep you informed, and what to do if you are not satisfied with our answer.
- **Right to Lodge a Complaint with the Regulator:** You may lodge a complaint with the Information Commissioner's Office (ICO) at ico.org.uk or by calling 0303 123 1113.

Where you are under 18, you may exercise these rights yourself, and a parent or guardian may also contact us on your behalf. To exercise any of these rights, please contact us at main@thesportingnetwork.com. We will respond within one calendar month. Where a request is complex, or where we need further information from you in order to respond, we will inform you and the time limit may be extended or paused in accordance with applicable law.

1.13

Data Security

We implement appropriate technical and organisational measures to protect personal data, including:

- Encrypted data transmission using TLS/HTTPS
- Secure password hashing using industry-standard algorithms
- Role-based access controls and the principle of least privilege
- Regular security assessments and vulnerability testing
- Monitoring and logging of access to systems containing personal data
- Incident response procedures and breach notification processes

No method of electronic storage or transmission is completely secure. While we strive to protect your data, we cannot guarantee absolute security.

1.14

Data Breach Notification

In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach where required, notify affected individuals without undue delay where the breach is likely to result in a high risk,

and document all personal data breaches including facts, effects, and remedial action taken.

1.15

Automated Processing and Automated Decision-Making

Five automated processes operate on the Platform. None of them makes a decision producing legal or similarly significant effects on you.

PROCESS

WHAT IT DOES, AND WHAT IT CANNOT DO

Identity verification

Our provider, Persona, uses automated technology to compare your government-issued identity document with a live selfie and detect fraudulent documents. **A failed automated check is not final:** you may retry verification, and you may contact us at main@thesportingnetwork.com to request human review of the outcome.

Message checks

All messages are screened against a list of prohibited terms before delivery, and contact-request introductions are screened for links, social media handles and telephone numbers. A message caught by these checks may be blocked or flagged for review. No person reads your messages as part of this process, and no message content is sent to a third party. See section 1.7. If a message of yours is blocked and you believe that is wrong, contact us and we will look at it.

Automatic hiding of reported posts

Where three separate users report the same post, it is hidden from view before a person has reviewed the report. This control **can only hide a post** — it can never delete content, warn a user, or ban an account. Reports we have already dismissed do not count towards the three. A director then reviews and either restores the post or decides on a further outcome. You may ask us to look at it straight away rather than waiting.

Report prioritisation

When content is reported, an automated classifier provided by Anthropic assesses the report and suggests a category, an urgency, and whether a young person may be at risk, so that we look at the most serious reports first. **This classification is advisory only.** It does not remove content, restrict an account, or produce any other outcome by itself — every report is reviewed and decided by a member of our team.

Feed ranking

Posts in your feed are ordered using embeddings of public posts (from their text and, where the author has agreed, a written description of their photos or video still), your engagement record over the last 90 days, your feed preference profile, and six platform-wide weights recalculated nightly. See section 1.7(c). **This only changes the order in which posts appear to you.** It does not remove or hide content, limit who can see your posts, or affect your account, and it is not used for advertising. For users under 18, personalised ordering is off unless they switch it on.

We do not make decisions producing legal or similarly significant effects on users by solely automated means. Feed ranking involves profiling, as described at section 1.7(c), but it has no legal or similarly significant effect, and we carry out no other profiling. If this changes in the future, we will update this Policy and, where required, obtain your explicit consent.

1.16

Identity Verification

Identity verification is performed by our specialist provider, Persona, which collects images of your government-issued identity document and a live selfie and uses biometric facial comparison to confirm that you are the document holder.

Verification is not required to create an account, build a profile, or use the Platform generally. It is required in the following circumstances:

- Where an account registered as a coach, scout, club, academy or team wishes to **start a new conversation with any user** on the Platform
- Where a coach or scout wishes to use **scout search**, which allows athletes to be searched and filtered, including by location
- Where any user wishes to display a **verified badge** on their profile

We apply these requirements because scout search allows young athletes to be identified and filtered at scale, and because opening a conversation with a young athlete is the point at which contact begins. We consider identity verification a proportionate safeguard on both. Ordinary search of the Platform does not require verification.

If you hold an athlete account, declining verification does not restrict your use of the Platform in any way — you can build a full profile, be discovered, post content, join teams and use messaging as normal. The only thing you do not get is a verified badge. If you hold a coach, scout, club, academy or team account and decline verification, you cannot start a new conversation with any user and you cannot use scout search; other features remain available to you.

Users under 18 may choose to complete identity verification, and some do so in order to display a verified badge. It is never required for a user under 18, and biometric processing takes place only where explicit consent has been given (see section 1.5). Where a user under 18 wishes to verify, we encourage them to discuss it with a parent or guardian first.

Your identity document and selfie are collected by and stored with Persona, not with us. We never receive or hold copies of these images or the biometric data derived from them — we receive only the outcome of the verification (e.g. approved or declined) and limited metadata needed to link that outcome to your account. Persona processes and stores this data on our behalf under a data processing agreement, retains it in accordance with its retention schedule and applicable law, and deletes it thereafter. Persona's own privacy practices are described in its privacy policy at withpersona.com/legal/privacy-policy.

Verification confirms identity only. It is not an endorsement of any user's sporting credentials, qualifications, conduct, or suitability to work with or contact others, including minors. We do not carry out criminal record or barred-list checks on any user. Verification also confers no additional visibility: a private account, and every account held by a 13–17 year old that has not been made public, is invisible to a verified coach or scout exactly as it is to any other non-connection.

1.17

Changes to This Policy

We may update this Privacy Policy from time to time. Where changes are material, we will notify users by email, in-app notification, or a prominent notice on the Platform. The "Last Updated" date at the top indicates when it was most recently revised. Continued use of the Platform after changes take effect

constitutes acceptance of the revised Policy.

1.18

Contact Us

The Sporting Network LTD

14 Hollywell Row, London, England, EC2A 4JB

Email: main@thesportingnetwork.com

Supervisory Authority: Information Commissioner's Office (ICO), ico.org.uk

Version History

VERSION	DATE	CHANGE
2.0	1 April 2026	Previous version.
2.1	24 August 2026	Health and fitness data identified as special category data with an Article 9(2) (a) explicit consent condition. Anthropic added as a processor covering the AI assistant, moderation triage, and translation. Third parties separated into processors and independent controllers. PostHog removed. Maps and location providers corrected. Under-18 protections restated to describe full account privacy, field-level privacy, the absence of shareable profile links, and optional identity verification. Automated decision-making section expanded to describe advisory moderation triage, and the categories of data sent for triage identified. Retention by our AI provider stated. Transfer safeguards for Anthropic named specifically. Sub-processor obligations added. Moderation record retention clarified. Account deletion path corrected.
2.2	26 August 2026	Section 1.3 now records that accounts held by users aged 13–17 are private by default. Section 1.7 restructured to disclose the automated checks applied to all messages before delivery, separately from the circumstances in which a person reads message content. Section 1.15 rewritten to cover all four automated processes, adding the message checks and the automatic hiding of a post reported by three separate users. Section 1.8 updated accordingly. Verification is recorded throughout as gating the starting of a new conversation as well as scout search, with the effect of declining stated separately for athlete and for coach, scout and team accounts. Article 9(2)(g) recorded as the fallback condition for biometric data, with the Appropriate Policy Document noted. Retention of the verification outcome stated. Complaint timescale aligned to the Complaints Procedure.
2.3	18 September 2026	Personalised feed ranking disclosed. OpenAI added as a processor for post embeddings, with what is and is not sent stated, including that nothing written by users under 18 is sent. New section 1.7(c) describes the engagement record (90-day automatic deletion), the per-user feed preference profile, and the nightly platform-wide weights, and records that feed ranking is profiling without legal or similarly significant effect, applying to users under 18. Nothing written by a user under 18, personal or team, is sent, and an account without a confirmed date of birth is treated as under 18. For users under 18 the feed is ordered using a starting profile based on the sports on the profile. Section 1.4 adds feed engagement data and a new category of derived information. Legitimate interests, retention, international transfers (OpenAI safeguards named), the right to object, and the under-18 protections updated accordingly. Section 1.15 now covers five automated processes.

2.4	18 September 2026	Media analysis for feed ranking disclosed: photos and video stills in public posts are described by Anthropic where the author has agreed, and the description is included in the text embedded by OpenAI. Agreement is asked for before the first public media post and can be withdrawn in Settings, deleting the descriptions. Nothing uploaded by a user under 18 is sent. Under-18 feed personalisation corrected: personalised ordering is off by default for under-18s and no engagement record is kept unless they switch it on. The adult post-ranking notice and Settings control are now described. Sections 1.3, 1.4, 1.6, 1.7(c), 1.9, 1.10, 1.12 and 1.15 updated.
2.5	18 September 2026	Retention of photos and video stills sent to Anthropic for feed ranking corrected: they are retained for up to 30 days for abuse monitoring and then deleted, on the same terms as the AI assistant, replacing the zero-data-retention wording. The feed engagement record and feed preference profile are now stated consistently as kept or built only where personalised ordering is on, and as deleted immediately when personalisation is switched off. Sections 1.4, 1.7(c) and 1.9 updated.
2.6	18 September 2026	Error and crash reporting disclosed: Sentry added as a processor receiving technical error reports from the app and website, with what a report contains and does not contain stated, sent only from accounts held by users aged 18 and over, processed in the European Union. Retention of error reports stated. Sections 1.9 and 1.10 updated.

The Sporting Network Ltd · Company number 16989082 · Registered office: 14 Hollywell Row, London, EC2A 4JB · ICO registration ZC110454

Privacy Policy v2.6 · Effective 18 September 2026 · Published at thesportingnetwork.com/privacy