



Safeguarding Policy

How we protect children and young people who use The Sporting Network.

VERSION	1.1
EFFECTIVE FROM	26 August 2026
LAST UPDATED	26 August 2026
APPROVED BY	Board of Directors, The Sporting Network LTD, 26 August 2026
POLICY OWNER	Charles Heffron, Director and Designated Safeguarding Lead
NEXT REVIEW	26 August 2027, or sooner following a significant change or incident
PUBLISHED AT	thesportingnetwork.com/safeguarding

6.1 Statement of Commitment

The Sporting Network LTD operates a platform used by children and young people. We accept that this brings responsibility, and we treat the safety and wellbeing of young users as our first consideration in how the Platform is designed and run.

We are committed to the principle that the welfare of a child is paramount, that all children have an equal right to protection from harm regardless of age, sex, disability, race, religion, gender identity or sexual orientation, and that safeguarding is everyone's responsibility — not only that of the Designated Safeguarding Lead.

We recognise that a platform which allows adults to search for and contact young athletes carries inherent risk. This Policy exists to identify that risk honestly and to set out what we do about it.

6.2 Scope and Definitions

This Policy applies to all directors, employees, contractors, volunteers, ambassadors and anyone acting on behalf of The Sporting Network LTD, and to all activity on our web platform, our mobile applications, and our social media channels.

Our minimum age is 13. Users aged 13–17 are treated as children for the purposes of this Policy.

- **Child / young person** — anyone under the age of 18, regardless of whether they are considered an adult in the country where they live.
- **Safeguarding** — protecting children from maltreatment, preventing impairment of their health or development, and taking action to enable all children to have the best outcomes.
- **Designated Safeguarding Lead (DSL)** — the named person with lead responsibility for safeguarding within the Company.

6.3 Legal and Regulatory Framework

This Policy is written with regard to:

- The Children Act 1989 and Children Act 2004
- Working Together to Safeguard Children (statutory guidance)
- The Online Safety Act 2023 and Ofcom's Protection of Children Codes of Practice
- The UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025
- The ICO's Age Appropriate Design Code (the Children's Code)
- The Sexual Offences Act 2003, including offences of sexual communication with a child and meeting a child following sexual grooming

6.4 Roles and Responsibilities

ROLE	NAMED PERSON	RESPONSIBILITY
------	--------------	----------------

Designated Safeguarding Lead	Charles Heffron Director	Overall responsibility for safeguarding. Receives and assesses all safeguarding concerns, decides on action, makes referrals to police, CEOP or children's social care, maintains safeguarding records, and reports to the Board.
Deputy Safeguarding Lead	Daniel Lindley Director	Acts with the full authority of the DSL whenever the DSL is unavailable. Must not delay action pending the DSL's return where a child may be at risk.
The Board	All directors	Approves this Policy, reviews safeguarding as a standing agenda item, and ensures adequate resource is given to it.
All personnel	Everyone	Must report any safeguarding concern to the DSL immediately. No one is expected to decide whether a concern is serious enough — that judgement belongs to the DSL.

Safeguarding contact: main@thesportingnetwork.com. Concerns raised through this address are seen by the DSL and Deputy DSL.

Availability. Both named leads are university students and there will be periods when one is genuinely unavailable, including during examinations. Cover is not optional: where the DSL cannot act within the timescales in section 6.9, the Deputy DSL must act. Where both are unavailable for a foreseeable period, cover arrangements must be agreed and recorded in advance.

6.5 How the Platform Is Designed to Protect Young Users

Safeguarding on an online platform is delivered primarily through product design, not through policy documents. The following controls are built into the Platform:

- **Under-18 accounts are private by default.** A young person is visible to the wider Platform only if they choose to be.
- **A private account cannot be seen by anyone who is not an accepted connection.** It does not appear in any search, it cannot be reached by visiting a link, and no account type — including a verified coach or scout — can see past it.
- **Under-18 accounts cannot share a profile link at all.** An under-18 profile exists only inside the Platform and cannot be circulated outside it.
- **Every user can make individual fields private** without making their whole account private.
- **Discoverability does not permit contact.** An adult who finds a young athlete's profile cannot reach them directly: any message from a user they are not connected with lands in a request inbox and does not become a conversation unless the young person accepts it.
- **Discoverability at scale is gated.** Scout search — the filtered search of athletes, including by location — requires identity verification, so an unverified adult cannot systematically identify young athletes by area.
- **Date of birth is never displayed publicly.**
- **Precise location is not published;** location is optional and coarse.
- **Reporting is available on every surface,** and reports involving a young person are prioritised.

6.6 Recorded Decision: Profile Visibility Default for Users Aged 13–17

Accounts held by users aged 13–17 are private by default. Accounts held by users aged 18 and over are public by default. The young person may make their profile public at any time, and may make it private again at any time.

What "private" means on this Platform

A private account is not visible to anyone the account holder has not accepted as a connection. Specifically:

- **It cannot be seen.** A private profile is not visible to other users of the Platform, to coaches or scouts, or to search engines.
- **It cannot be found.** A private account does not appear in search of any kind, including scout search. There is no way to filter, browse or otherwise arrive at a private profile.
- **It cannot be visited directly.** There is no link that will open a private profile for someone who is not a connection, and a private account's profile link cannot be shared.
- **No account type can bypass it.** Identity verification does not confer the ability to see past a privacy setting. A verified coach or scout sees exactly what any other non-connection sees, which is nothing.

Privacy on this Platform is a restriction on access, not a request to be left alone.

Under-18 profiles cannot be shared outside the Platform

An account held by a user aged 13–17 cannot generate or share a profile link, in any visibility state. This applies whether the young person's account is private or public, and there is no setting that turns it on.

The effect is that an under-18 profile exists only inside SportNet. It can be seen by people using the Platform, and it cannot be sent, posted or circulated anywhere else. A young person's profile cannot be forwarded into a group chat, embedded in a website, or passed to someone who does not hold an account. Adult accounts can share a profile link; under-18 accounts cannot.

Field-level privacy, for every user

Every user, of any age, can set individual parts of their profile to private without making the whole account private. Physical metrics, posts, achievements, academic grades and other elements can each be restricted on their own while the rest of the profile stays visible.

This means a young person who wants to be discoverable does not have to choose between being fully visible and being invisible. They can be found for their sport while keeping the details they would rather not publish out of view. These controls apply on public and private accounts alike and, like the account-level setting, cannot be bypassed by any account type.

Rationale for the default

This decision applies the Children's Code standard that settings be high privacy by default for children, and that any reduction in privacy be the result of a deliberate action by the child rather than the starting position.

It is recorded here because it is the most significant safeguarding decision in the design of the Platform, and because the trade-off it makes is real. The purpose of the Platform is to allow athletes to be discovered and to access sporting opportunities they would not otherwise reach — university and scholarship routes, clubs, academies and trials. A profile that is private cannot be discovered. We have nonetheless concluded that a young person should choose to

be discoverable rather than be made discoverable, and that the cost of that choice being an active one is a cost the Platform should bear rather than the child.

The previous version of this Policy recorded the opposite decision, on the basis that a private default would disproportionately disadvantage young athletes without existing contacts or the means to pay for representation. That concern remains real, and it is addressed by making the control prominent, explained in age-appropriate language at the point of registration, and reversible at any time — rather than by making the exposure automatic.

Protections that apply regardless of the setting chosen

- No shareable profile link for under-18 accounts, in any visibility state.
- Field-level privacy controls, on public and private accounts alike, unby-passable by any account type.
- Date of birth is never displayed publicly.
- Advertising identifiers are not collected from under-18 accounts, and analytics are switched off entirely for them. We do not use children's data to target advertising.

Mitigations relied upon where a young person chooses to be public

Where a young person makes their profile public, the following controls limit what that discoverability actually exposes them to:

- **Minimum age of 13**, enforced at registration through a date-of-birth age gate. Accounts identified as belonging to under-13s are deleted.
- **Identity verification gate on scout search.** A coach or scout must complete identity verification through Persona before they can use scout search — the filtered search of athletes, including searching by location. An unverified account cannot identify and filter young athletes at scale.
- **Request inbox.** No user can hold a conversation with a young athlete they are not connected with. Any message from an unconnected user goes to a request inbox, and does not reach their main conversations unless the young person accepts it. A young person is never required to engage, and can ignore or decline any approach.
- **Reporting on every surface** — profiles, posts, comments and messages can all be reported, by any user, including users who are not the person affected.
- **Proactive review.** Where we have reason to believe a young user is at risk, we may review interactions involving that user, including message content.

Review

This decision must be reviewed at each annual review of this Policy, and immediately following any incident in which profile visibility was a contributing factor.

This decision is the most significant safeguarding trade-off in the design of the Platform. We record it openly, with our reasoning, so that it can be scrutinised and challenged — by our users, by parents, and by regulators. If you think we have it wrong, tell us at main@thesportingnetwork.com.

6.7 Risks We Are Alert To

The principal safeguarding risks on a platform of this kind are:

- **Grooming** — an adult building trust with a young person with the intention of abusing or exploiting them, including by posing as a coach, scout or agent.
- **Misuse of the scouting relationship** — using a position of apparent authority or the promise of a sporting opportunity to obtain compliance, images, money or a private meeting.
- **Moving contact off-platform** — pressing a young person onto messaging apps or social media where our controls do not apply. This is a recognised grooming indicator and is prohibited by our Community Guidelines.
- **Requests for images** — including requests framed as sporting assessment, such as physique, weight or body-composition photographs.
- **Requests to meet** — arranging trials, sessions or meetings without the involvement of a parent, guardian or club.
- **Child sexual abuse material** — the uploading, sharing or solicitation of indecent images of children.
- **Bullying and harassment** between young users, including within teams and group messaging.
- **Content harmful to young people**, including material promoting self-harm, suicide, disordered eating, or unsafe training, weight-cutting or supplement use.
- **Financial exploitation** — fraudulent agents, trial fees, or scholarship scams targeting young athletes and their families.

6.8 How Concerns Reach Us

A safeguarding concern may arrive through any of the following routes, and all are treated equally seriously:

- A report made by a user through the in-app reporting tools
- An email to main@thesportingnetwork.com, including from a parent, guardian, school, club or governing body
- Something identified by a director or member of the team during normal work on the Platform
- Contact from the police, CEOP, a local authority or another safeguarding body
- A disclosure made directly to us by a young person

You do not need to hold an account to raise a safeguarding concern with us, and you do not need to be certain that something is wrong before reporting it.

6.9 Responding to a Concern

Where a concern involves a risk of harm to someone under 18, the DSL or Deputy DSL will:

- **Act on the same day.** Safeguarding concerns are not held for the standard 72-hour review window.
- **Take immediate protective action** — which may include removing content, terminating the account concerned, and preventing further contact with the young person.
- **Preserve evidence.** Relevant records, including message content, account details and reporting history, must be preserved and not deleted, so that they are available to the authorities. Removing content from public view is not the same as destroying it.

- **Refer externally** in accordance with section 6.10.
- **Record the concern**, the assessment, the action taken, the reasoning and the outcome, contemporaneously.

Where there is any doubt about whether a matter should be referred, the presumption is to refer. It is not our role to investigate whether abuse has occurred, or to interview a suspected perpetrator. Our role is to act protectively, preserve evidence and pass the matter to those with the authority to investigate.

We may act without notifying the user concerned, and without their consent, where notification would place someone at risk or prejudice an investigation.

6.10 External Referral

SITUATION	REFERRAL ROUTE
A child is in immediate danger	Police — 999. Make the call first, then record it.
Online child sexual abuse, exploitation, or grooming	CEOP (Child Exploitation and Online Protection Command) at ceop.police.uk , and the police on 101 where not an emergency.
Suspected child sexual abuse material on the Platform	Internet Watch Foundation at iwf.org.uk and the police. Content must be removed from view, preserved for law enforcement, and never downloaded, copied or forwarded by our team.
Concern about a child's welfare, not an emergency	Children's social care at the local authority for the area where the child lives. Where the child's location is unknown, refer to the police on 101.
Concern involving a coach, scout or club affiliated to a governing body	The safeguarding team of the relevant national governing body, in addition to any police or local authority referral.
Advice needed, no referral decision yet	NSPCC Helpline — 0808 800 5000. The NSPCC will advise without requiring a formal referral.

Referring a matter externally does not end our responsibility. We continue to act protectively on the Platform and to cooperate with any investigation.

6.11 Allegations About a Director or Someone Working for Us

Where an allegation is made that a director, employee, contractor, volunteer or ambassador has harmed a child, behaved towards a child in a way that indicates they may pose a risk, or behaved in a way that indicates they may be unsuitable to work with children:

- The allegation must be reported to the other director immediately, and must not be handled by the person against whom it is made.
- The person concerned must be removed from any access to safeguarding records, moderation tools, user data and young users pending the outcome.

- The matter must be referred to the Local Authority Designated Officer (LADO) for the relevant area and, where a criminal offence may have occurred, to the police.
- The Board must be informed.

Where an allegation concerns the DSL, the Deputy DSL assumes full responsibility for handling it, and vice versa.

6.12 Safer Conduct by Our Team

Anyone acting for the Company must:

- Never contact a young user privately through personal accounts or off-platform channels
- Never arrange to meet a young user alone
- Never ask a young user for images, personal contact details, or information beyond what the Platform requires
- Keep all communication with young users on the Platform or through official Company channels, so that it is recorded
- Report any concern immediately, including concerns about the conduct of a colleague

Access to user data, message content and moderation tools is restricted to the directors named in section 6.4 and is granted on a least-privilege basis. Access is not a general entitlement, and access to a young person's data must have a specific, recorded purpose.

6.13 Content, Filming and Marketing Involving Under-18s

Where we produce, commission or publish content featuring anyone under 18 — including video, photography, interviews, testimonials and ambassador content:

- Written parental or guardian consent must be obtained before filming and before publication, and must be retained.
- Where filming takes place at a school, club or other organisation, we work to that organisation's own safeguarding and consent procedures, and do not substitute our own.
- Content must not identify a young person's school, club, training times or location in a way that would allow them to be found.
- Consent may be withdrawn, and we will remove content from our own channels on request.

6.14 Competence and Awareness

Before handling any report, the DSL and Deputy DSL must be familiar with this Policy, with the Safeguarding Referral and Escalation Procedure at Annex A, and with the indicators of grooming and online exploitation set out in section 6.7.

Where either lead is uncertain whether a matter should be referred, they must seek advice rather than decide alone. The NSPCC Helpline (0808 800 5000) provides advice without requiring a formal referral. The presumption throughout is to refer.

The Board keeps under review whether formal safeguarding training should be undertaken, taking account of the size of the Platform, the volume of reports received, and any requirement arising from a partner organisation or regulator.

Anyone joining the Company in a role with access to user data or moderation tools must read this Policy and confirm they have understood it before that access is granted.

6.15 Records and Confidentiality

Safeguarding records are held securely and separately from general business records, are accessible only to the DSL and Deputy DSL, and are retained in line with our data retention schedule and any legal hold.

Safeguarding information is shared on a need-to-know basis. We will share information with the police, children's social care or another safeguarding body without the consent of the individual concerned where it is necessary to protect a child. Data protection law does not prevent the sharing of information for safeguarding purposes.

6.16 Review

This Policy is reviewed annually by the Board, and additionally following any safeguarding incident, any significant change to the Platform, or any change in law or regulatory guidance. Safeguarding is a standing item at every board meeting.

Version history

VERSION	DATE	CHANGE
1.0	August 2026	First issue. Not published.
1.1	26 August 2026	First published version. Section 6.6 records under-18 accounts as private by default, and sets out what a private account means, the restriction on sharing under-18 profile links outside the Platform, and the field-level privacy controls available to all users. Section 6.5 updated accordingly.

6.17 Contact

- Designated Safeguarding Lead: Charles Heffron — main@thesportingnetwork.com
- Deputy Safeguarding Lead: Daniel Lindley — main@thesportingnetwork.com
- The Sporting Network LTD, 14 Hollywell Row, London, England, EC2A 4JB

The Sporting Network Ltd · Company number 16989082 · Registered office: 14 Hollywell Row, London, EC2A 4JB · ICO registration ZC110454
Safeguarding Policy v1.1 · Effective 26 August 2026 · Published at thesportingnetwork.com/safeguarding