



Data Protection Policy

Internal governance and operational requirements for protecting personal information

Strive PE and Sport Ltd

Version: 1

Effective date: September 2026

Last review: September 2026

Next scheduled review: September 2027

This internal policy sets out how Strive PE and Sport Ltd manages and protects personal information and demonstrates compliance with applicable UK data protection law. It should be read alongside the public-facing Privacy Notice, which explains our processing to individuals.

1. Purpose and commitment

Strive PE and Sport Ltd ("Strive", "we", "us" or "our") is committed to protecting personal information and handling it lawfully, fairly, securely and transparently. This policy combines our internal data protection arrangements with the privacy information we provide to individuals whose personal data we process.

As an organisation delivering sport, education, childcare and community activities, including services involving children and young people, we recognise the additional risks and responsibilities associated with children's information. We will apply a high standard of privacy, take the best interests of children into account as a primary consideration where relevant, and collect only information that is adequate, relevant and necessary.

This policy is intended to operate with the UK GDPR, Data Protection Act 2018 (as amended), Data (Use and Access) Act 2025 ("DUAA"), Privacy and Electronic Communications Regulations 2003 ("PECR"), applicable safeguarding requirements and other relevant legislation and regulatory guidance.

2. Scope

This policy applies to personal information processed by Strive in electronic, paper, verbal or other forms, including information processed through booking platforms, payment providers, cloud systems, schools, local authorities and other suppliers.

- Children and young people;
- Parents, carers and guardians;



- Employees, volunteers, coaches, contractors and applicants;
- Schools, academies and educational settings;
- Partner organisations, suppliers and professional advisers;
- Website visitors, enquirers, customers and participants;
- Any other individual whose personal data Strive processes.

3. Data controller and processor roles

Strive PE and Sport Ltd is generally the data controller where it determines why and how personal data is processed, including for its own bookings, programmes, administration, safeguarding and business operations.

Where Strive processes personal data solely on behalf of a school, local authority or another organisation, the other organisation may be the controller and Strive may be a processor. In those circumstances Strive will follow the applicable written data processing agreement and the controller's lawful instructions, subject to legal requirements. We will not assume that we are always the controller simply because we hold the information.

4. Organisation and contact details

Strive PE and Sport Ltd is a private limited company registered in England and Wales, company number 12479339.

Registered office: 34 Crosier Court, Upchurch, Kent, ME9 7AR

Email: admin@strivepeandsport.co.uk

Parent line: 07378 951411

5. ICO registration / data protection fee

Where Strive is required to register with the Information Commissioner's Office (ICO) and pay the data protection fee, we will maintain that registration and keep the details in this notice accurate. If an exemption applies, we will document the basis for the exemption.

ICO registration/fee reference: [INSERT CURRENT ICO REGISTRATION NUMBER / CONFIRM EXEMPTION BEFORE PUBLICATION]. This field must not remain as a placeholder when the policy is published.

6. Data protection governance and responsibilities

The Directors have overall responsibility for ensuring that this policy is implemented and reviewed. Strive will designate a Data Protection Lead to coordinate day-to-day compliance, rights requests, breach management and liaison with the ICO where appropriate.



A formal Data Protection Officer (DPO) will be appointed if Strive becomes legally required to have one. The requirement will be assessed periodically, including whether core activities involve large-scale regular and systematic monitoring or large-scale processing of special category data or criminal-offence data.

- Staff, volunteers and contractors must follow this policy and only access information necessary for their role.
- Suspected data breaches must be reported immediately.
- Managers must ensure staff receive appropriate data protection and confidentiality training.
- New or materially changed processing must be assessed for privacy risks before implementation.

7. Data protection principles

Strive will comply with the UK GDPR principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. We will be able to demonstrate compliance through appropriate policies, records, contracts, training, risk assessments and other documentation.

8. Information we collect

The information collected depends on the service and relationship with Strive. It may include:

- Names, dates of birth, age/year group and school or educational setting;
- Parent/carers contact details, address and emergency contact information;
- Booking, attendance, participation and programme records;
- Payment and billing information and transaction references;
- Medical, allergy, dietary, disability, SEND and additional support information where necessary;
- Accident, incident, first-aid and safeguarding records;
- Behavioural information where necessary and proportionate;
- Consent and preference records, including photography and marketing choices;
- Employment, recruitment, qualification, training, right-to-work and DBS-related information;
- Website, device, IP address, cookie and usage information;
- Correspondence, complaints, feedback and survey responses;
- Photographs and videos where a lawful basis permits their collection and use.

Emergency contact information is personal data but is not itself special category data. Health, allergy and disability information may constitute special category data and requires an Article 9 condition in addition to an Article 6 lawful basis.

9. Children and young people

We recognise that children's personal information requires particular care. We will consider the child's age, understanding, vulnerability and the nature and risks of the processing.



- Use clear, age-appropriate explanations where children are themselves the audience for privacy information or controls.
- Consider the best interests of the child as a primary consideration where applicable.
- Do not use children's information in ways that are detrimental to their wellbeing.
- Apply high-privacy defaults and appropriate access controls.
- Take particular care before sharing children's information with third parties and document the reason for material or higher-risk sharing.
- Carry out a Data Protection Impact Assessment (DPIA) where required and consider one where processing presents significant risks to children.

Where parents or carers provide information on behalf of children, we will not treat parental consent as a universal substitute for the child's rights. The appropriate lawful basis, transparency requirements and, where relevant, the child's own rights will be considered for each processing activity.

10. How and when we collect information

- Enquiries, registrations and bookings;
- Online forms and booking systems;
- Attendance at activities and events;
- Telephone, email, social media or other communications;
- Schools, local authorities and partner organisations where information is lawfully shared;
- Employment and volunteering applications;
- Safeguarding, medical, accident or emergency processes;
- Website visits and online technologies;
- Marketing subscriptions or other communications where lawful.

Where information is obtained from another organisation rather than directly from the individual, we will consider the applicable transparency requirements and any exemption that may apply.

11. Purposes of processing

- Provide and administer booked services and programmes;
- Manage registrations, attendance, waiting lists and payments;
- Communicate with parents, carers, schools and participants;
- Protect health, safety and welfare and respond to emergencies;
- Safeguard children and vulnerable individuals;
- Make and record reasonable adjustments and inclusion arrangements;
- Record and investigate accidents, incidents and complaints;
- Meet legal, regulatory, contractual and funding obligations;
- Recruit, employ, train and manage staff and volunteers;
- Prevent fraud, misuse and security incidents;
- Evaluate and improve services;



- Produce appropriate statistics and reports, preferably anonymised or aggregated where practicable;
- Protect our legal rights and interests and obtain professional advice where necessary.

12. Lawful bases – ordinary personal data

For each processing activity Strive will identify and document the applicable Article 6 lawful basis.

Depending on the circumstances this may include:

- Contract – where processing is necessary to enter into or perform an agreement.
- Legal obligation – where processing is necessary to comply with a legal obligation.
- Legitimate interests – where processing is necessary for a legitimate interest pursued by Strive or a third party, except where the individual's interests or fundamental rights and freedoms override that interest.
- Consent – where consent is the appropriate lawful basis. Consent must be freely given, specific, informed and unambiguous, evidenced by clear affirmative action, and capable of being withdrawn.
- Vital interests – in exceptional circumstances where processing is necessary to protect someone's life.
- Public task – only where Strive is actually performing a task in the public interest or under official authority and the relevant legal basis applies.

A single lawful basis will not automatically apply to all processing carried out under a particular service.

13. Special category data

Health information, allergies, disability information and some SEND information are special category data where they fall within the relevant UK GDPR definition. Special category processing requires both an Article 6 lawful basis and an Article 9 condition.

Strive will identify the appropriate condition for the specific processing. Depending on the circumstances this may include explicit consent, employment/social protection law, vital interests, or a substantial public interest condition where the legal requirements are met. We will not describe all medical information as being processed solely on the basis of consent.

Where a Schedule 1 condition under the Data Protection Act 2018 is relied upon, Strive will maintain any required Appropriate Policy Document and supporting records.

14. Consent

Where consent is used, it will be separate from acceptance of terms and conditions wherever necessary and will not be made a condition of receiving a service unless the processing is genuinely necessary for that service.

- Consent requests will be clear and specific.
- Pre-ticked boxes will not be used.



- Different purposes, such as marketing and photography, will be separated where appropriate.
- We will keep records of who consented, what they consented to, when, how and the information provided at the time.
- Withdrawal will be as easy as giving consent.
- Withdrawal will not affect processing already carried out lawfully before withdrawal.

For safeguarding, emergency response and essential service delivery, Strive will not rely on consent where another lawful basis is more appropriate or where information may lawfully be processed without consent.

15. Photography and video

Photography and video involving identifiable children or other participants will be handled under a documented lawful basis. Where consent is used, it will be separate, optional and recorded. Images will only be used for the purposes communicated at collection. Marketing/publicity uses will be kept distinct from operational or educational uses where appropriate.

Consent can be withdrawn for future use, subject to practical limitations such as material already printed, distributed or published by third parties. Staff will follow Strive's Photography and Media Consent Procedure and safeguarding requirements.

16. Direct marketing

Direct marketing by email, text, social media message or other electronic mail to individuals must comply with PECR as well as UK GDPR where personal data is involved.

- Normally, specific consent is required for electronic marketing to individual subscribers unless a valid PECR exception applies.
- The limited existing-customer soft opt-in may be used only where all statutory conditions are met, including direct collection of contact details, similar products/services, an opt-out at collection and a simple opt-out in every later message.
- Marketing consent must not be hidden in general terms and conditions.
- Marketing messages must identify Strive appropriately and provide a valid way to opt out.
- Suppression/opt-out records will be maintained so that objections are respected.

The charitable-purpose soft opt-in introduced by the DUAA applies only to qualifying charities. Strive PE and Sport Ltd will not rely on that provision unless it independently meets the legal requirements.

17. Sharing personal information

We may share personal data where there is a lawful basis and the sharing is necessary, proportionate and appropriately secure. Possible recipients include:

- Schools, academies and educational settings;



- Local authorities and funding bodies;
- Parents/carers or authorised representatives where appropriate;
- Healthcare professionals and emergency services;
- Police, Children's Social Care and other safeguarding agencies;
- Regulators and statutory bodies where required or permitted;
- Payment providers and booking platforms;
- IT, cloud, communications and other service providers acting as processors;
- Insurers, auditors and professional advisers;
- Other organisations where disclosure is required or permitted by law.

We will share the minimum information reasonably necessary. A safeguarding disclosure does not require consent where another lawful basis permits or requires the sharing. Material sharing arrangements will be documented.

18. International transfers

If personal data is transferred outside the UK or accessed from another country, Strive will comply with the UK GDPR international transfer rules. Depending on the circumstances this may include UK adequacy regulations, an International Data Transfer Agreement, an appropriate UK Addendum to EU Standard Contractual Clauses, or another legally recognised safeguard. Required transfer risk assessments and supplementary measures will be considered.

19. Data processors and suppliers

Before appointing a processor that will handle personal data for Strive, we will carry out proportionate due diligence and ensure a written contract contains the protections required by UK GDPR. Processors must act only on documented instructions unless law requires otherwise, maintain appropriate security, assist with rights and breach obligations, and return or delete information when required.

Key suppliers should be reviewed periodically, particularly booking, payment, cloud storage, email, website, analytics and communications providers.

20. Data security

Strive will implement appropriate technical and organisational measures proportionate to the risks, including where appropriate:

- Strong passwords and multi-factor authentication;
- Role-based access controls and need-to-know access;
- Encryption where appropriate;
- Secure cloud and booking systems;
- Device, endpoint, firewall and anti-malware protections;
- Secure paper storage and confidential disposal;



- Backups and recovery arrangements;
- Staff confidentiality obligations and training;
- Regular review of permissions and supplier security;
- Secure methods for sharing sensitive information.

No system can be guaranteed to be completely secure. Staff must report suspected weaknesses or accidental disclosures immediately.

21. Data Protection Impact Assessments (DPIAs)

Strive will carry out a DPIA before processing that is likely to result in a high risk to individuals' rights and freedoms, and will consider a DPIA for other higher-risk activities. Particular care will be taken where processing involves children, special category data, systematic monitoring, new technologies, large-scale data use, profiling or significant data sharing. Where a DPIA identifies an unmitigated high risk that cannot be addressed, Strive will seek ICO consultation where legally required before proceeding.

22. Data breaches and incident management

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include sending information to the wrong person, lost devices, cyber incidents, compromised accounts and inappropriate access.

- All staff, volunteers and contractors must report suspected or actual breaches immediately to the Data Protection Lead.
- Where a breach is likely to result in a risk to individuals' rights and freedoms, Strive will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it.
- Where a breach is likely to result in a high risk, affected individuals will be informed without undue delay unless a lawful exception applies.
- All breaches will be documented, including those not reported to the ICO.
- Lessons learned and preventative measures will be recorded.

23. Retention and disposal

Personal data will be retained only for as long as necessary for the purpose for which it was collected, taking account of legal, safeguarding, contractual, financial, insurance and limitation requirements. The periods below are normal operational targets, not permission to keep information indefinitely.

- Booking and registration records: normally 6 years after the relevant service/last attendance.
- Attendance records: normally 6 years, subject to funding and legal requirements.
- Parent/customer correspondence: normally 6 years where relevant to contractual, complaint or legal records; routine correspondence may be deleted sooner.
- Medical information: normally for the duration of the relevant programme or as long as necessary; longer retention may apply where linked to an accident, claim or safeguarding matter.



- Accident/incident records involving children: retained according to applicable insurance, limitation, risk and safeguarding requirements.
- Safeguarding records: in accordance with applicable safeguarding guidance, legal requirements and Strive's safeguarding retention schedule.
- Financial records: normally 7 years, or longer where a documented legal, tax, audit or other requirement applies.
- Staff personnel records: normally 6 years after employment ends, subject to the nature of the record and legal requirements.
- Unsuccessful recruitment records: normally 6 months unless a longer period is justified and documented.
- DBS information: kept only in accordance with applicable law and the DBS Code of Practice; certificates will not be retained unnecessarily.
- Training records: normally for the duration of employment/engagement plus 6 years where appropriate.
- Photographs/videos: retained while needed for the stated purpose and subject to the applicable lawful-basis arrangements.
- Website enquiries: normally up to 2 years unless a longer period is justified.

These periods must be supported by a maintained Data Retention Schedule. Where a matter is subject to a complaint, claim, investigation, safeguarding process, legal hold or regulatory requirement, deletion may be suspended for relevant information until the matter is resolved.

24. Individual rights

- Be informed about processing;
- Access personal data;
- Rectify inaccurate or incomplete information;
- Erase personal data in certain circumstances;
- Restrict processing in certain circumstances;
- Object to processing based on legitimate interests, public task or direct marketing, as applicable;
- Receive certain personal data in a portable format where the requirements are met;
- Receive safeguards concerning certain automated decision-making/profiling;
- Withdraw consent where processing is based on consent.

These rights are not absolute. Safeguarding, legal obligations, legal claims and other exemptions may limit a right in particular circumstances.

25. Subject Access Requests and other rights requests

Requests should be sent to admin@strivepeandsport.co.uk or the registered office. A request does not need to use the words "Subject Access Request" and may be made verbally or in writing.

- We may carry out proportionate identity checks where necessary.



- We will respond without undue delay and normally within one month once the request can be processed.
- The period may be extended by up to two further months for complex or numerous requests where the law permits; the requester will be informed within the applicable initial period.
- Requests are normally free. A reasonable fee may be charged, or a request refused, only where the legal test for manifestly unfounded or excessive requests is met.
- We will consider the rights of other people and may redact third-party information where appropriate.
- Where a request is made on behalf of a child, we will consider the child's age, maturity, understanding, best interests and the circumstances before deciding what can be disclosed.

Staff receiving a rights request must forward it promptly to the Data Protection Lead.

26. Automated decision-making and profiling

Strive does not currently make decisions about individuals that have legal or similarly significant effects based solely on automated processing. If this changes, we will assess the applicable UK GDPR requirements before introducing the process, including safeguards, transparency, human intervention rights where required, and additional rules applying to children or special category data.

27. Cookies and similar technologies

Our website and online services may use cookies and similar storage/access technologies. We will maintain a current cookie notice or cookie policy identifying the technologies used, their purposes, providers, duration and relevant privacy information.

- Strictly necessary technologies may be used where an applicable PECR exemption permits them.
- Non-essential analytics, advertising, tracking or preference technologies will not be placed or accessed where PECR requires consent until valid consent has been obtained.
- Consent mechanisms will provide a genuine choice and will not rely on pre-ticked boxes or misleading design.
- Users will be able to change or withdraw cookie choices through available cookie controls.

The website team must review the actual cookies and scripts in use periodically. This policy is not a substitute for a current cookie scan and cookie-specific notice.

28. Safeguarding and information sharing

Safeguarding takes priority where a child or vulnerable person may be at risk. Strive may collect, use or share personal information without consent where this is necessary and lawful to protect a person from harm, comply with legal duties, cooperate with statutory safeguarding processes or protect vital interests. Staff must follow Strive's safeguarding and information-sharing procedures.



29. Complaints and ICO

Individuals should contact Strive first so concerns can be investigated and resolved where possible. If an individual remains dissatisfied, they may complain to the ICO.

Information Commissioner's Office (ICO): <https://ico.org.uk>

Telephone: 0303 123 1113

The ICO's current contact arrangements should be checked before publication rather than relying on an old postal address in this policy.

30. Training, monitoring and accountability

- Relevant staff will receive induction and refresher data protection training.
- Access permissions will be reviewed periodically and removed when no longer required.
- Data protection incidents, rights requests, complaints and material supplier issues will be recorded.
- Where legitimate interests are relied upon, appropriate assessments will be documented.
- Where consent is relied upon, evidence of consent and withdrawal will be retained.
- Records of processing activities will be maintained where required.
- DPIAs and supplier due diligence will be completed where appropriate.

31. Children's digital services

Where Strive provides an online service likely to be accessed by children, the service will be assessed against the ICO Children's Code and applicable UK GDPR/DUAA requirements. Privacy information and controls will be clear and age-appropriate, privacy will be high by default, and the best interests of children will be a primary consideration.

If Strive introduces profiling, targeted advertising, geolocation, online messaging, social features, age assurance or similar higher-risk processing involving children, a specific privacy and risk assessment will be completed before launch.

32. Policy review and change control

This policy will be reviewed at least annually and sooner where there is a material legislative, regulatory, technological or organisational change, a significant data breach, a new high-risk processing activity or a material change to the services Strive provides.

The Directors are responsible for ensuring that the published privacy notice matches actual processing. Website notices, booking forms, consent wording, cookie controls, staff procedures and supplier arrangements must be updated when necessary; the policy must not promise processing practices that are not actually implemented.



33. Related documents

- Safeguarding and Child Protection Policy
- Health and Safety Policy
- Safer Recruitment Policy
- Equality, Diversity and Inclusion Policy
- Staff Code of Conduct
- Information Security Policy
- Online Safety Policy
- Photography and Media Consent Procedure
- Data Retention Schedule
- Data Breach / Incident Response Procedure
- Data Subject Rights Procedure
- Data Processing Agreements
- Cookie Policy / Cookie Notice
- Direct Marketing Procedure

34. Approval

Approved by: Directors of Strive PE and Sport Ltd

Effective date: September 2026

Version: 4

Next scheduled review: September 2027

This document is intended to be a robust operational policy and privacy notice. It should be read alongside the organisation's actual processing arrangements, contracts, booking systems, cookie configuration, retention schedule and consent mechanisms. Where a particular processing activity creates significant legal or safeguarding risk, specialist legal advice should be obtained.