# GDPR Policy

**Date:** November 2025

**Next review due:** October 2026

This policy will be reviewed annually or earlier if legislation or statutory guidance changes. All staff must familiarise themselves with this policy and related procedures.

## 1. Policy Statement

At Kanga Sports Ltd ("the Company"), we are committed to protecting the personal data it handles and ensuring that all processing is carried out in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Kanga Sports Ltd aims to process personal data lawfully, fairly, and transparently, and to uphold the rights, privacy, and freedoms of all individuals whose data we process. The Company will maintain appropriate technical and organisational measure to safeguard personal data and will ensure that all staff, contractors, and third parties acting on its behalf understand and comply with these responsibilities.

# 2. Scope

This policy applies to all personal data processed by the Company in any format, including digital, paper-based, or any other recorded form. It applies to:

- All Kanga Sports employees, including apprentices, contractors, volunteers, work experience placements and senior members
- Customers, parents, children, and any service users
- Third parties providing services to or on behalf of the Company

The policy covers all processing activities undertaken by Kanga Sports Ltd, including the collection, storage, use, transfer, sharing, and disposal of personal data. It applies to all business functions, systems, platforms, and processes where personal data is handled.

# 3. Applicable Law

This policy is governed by and complies with the following legislation:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018**
- The **Privacy and Electronic Communications Regulations (PECR)**, where applicable
- Any relevant updates introduced by the **Data (Use and Access) Act 2025**

- Any other statutory obligations relating to data protection and privacy that apply within the United Kingdom

These laws set out the requirements for how the Company must collect, process, store, share, and protect personal data.

# 4. The Data Protection Principles

This policy continues to rest on the same fundamental data-protection principles as before, as required under UK GDPR (mirroring the former EU GDPR).

Personal data must be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary for the purposes for which it is processed
- Accurate and, where necessary, kept up to date (with rectification or erasure of inaccurate/incomplete personal data without delay)
- Kept in a form which permits identification of data subjects for no longer than necessary (unless retained longer for archiving, research or statistical purposes with appropriate safeguards)
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, via suitable technical and organisational measures.

# 5. Legal Bases for Processing

Under UK data protection law, personal data processing is lawful only if at least one of the following bases applies:

- Consent: the data subject has given clear, informed, free and specific consent for one or more purposes
- Performance: the processing is necessary to perform a contract to which the data subject is party, or to take steps at their request prior to contract formation
- Legal obligation: the processing is necessary to comply with a legal obligation to which the Company is subject
- Vital interests: to protect the life or safety of the data subject or another natural person

For sensitive ("special category") personal data (e.g. health, race, religion, etc) additional conditions apply under UK GDPR / DPA 2018. The Company will only process such data if one of the lawful conditions for special category data is met (for example, explicit consent, necessary for employment/social protection, vital interests, or other DPA-permitted exceptions).

# 6. Purpose Limitation & Data Minimisation

**6.1** The Company collect and processes personal data only for specified and legitimate purposes, and shall not further process it in a way incompatible with those purposes.

**6.2** Only personal data adequate, relevant and limited to what is necessary for those purposes will be collected and processed.

# 7. Accuracy and Keeping Data Up to Date

**7.1** The Company shall ensure personal data is accurate and kept up to date. At collection and periodically thereafter, the data should be reviewed, and any inaccurate or out-of-date data should be rectified or erased without undue delay.

**7.2** Data subjects may request rectification under their rights.

# 8. Data Retention

**8.1** Personal data shall not be kept for longer than necessary in light of the purposes for which it is collected and processed.

**8.2** When data is no longer required, it shall be securely erased or disposed of without undue delay.

**8.3** Where personal data is retained for longer (e.g. for archiving, statistical, or research purposes), the Company will implement appropriate safeguards.

# 9. Security of Processing

The Company shall implement appropriate technical and organisational measures to ensure the security of personal data - protecting against unauthorised or unlawful processing, accidental loss, destruction or damage.

Specific measures shall include:

- Secure storage of electronic data (e.g. encryption, access controls, secure servers), with regular backups stored off-site
- Secure storage of physical/hard-copy data (e.g. locked cabinets, restricted access)
- Secure methods for data transmission - e.g. encrypted networks, avoid unsecured networks, avoid transferring sensitive data over insecure or public means
- Internal policies to control who can access personal data, based on need-to-know
- Regular review of security measures, updating software/patches, ensuring password policies, and controlling access rights
- Training staff, volunteers, and contractors on data security and data-protection obligations

# 10. Accountability, Record-Keeping, & Governance

**10.1** The Company should appoint a Data Protection Officer (DPO), or designate a responsible person to oversee compliance with UK GDPR / DPA 2018.

**10.2** The Company shall maintain records of processing activities, including: identity of controller/processor, categories of personal data, categories of data subjects, purposes of processing, recipients (including third parties), transfers (especially outside the UK/EU), retention periods, and security measures implemented.

**10.3** Where the Company engages third-party processors, contracts must ensure that those processors implement equivalent data-protection and security obligations.

**10.4** All staff, volunteers, and contractors handling personal data must be trained, made aware of their responsibilities, and supervised.

# 11. Data Protection Impact Assessments

For any new project or new use of personal data (particularly where processing is likely to result in high risk to data subjects), the Company will conduct a Data Protection Impact Assessment (DPIA) covering: type of data, purpose of processing, necessity, proportionality, risks to data subjects and to the Company, and measures to mitigate risks.

# 12. Rights of Data Subjects

Under UK GDPR (and where applicable EU GDPR) data subjects have the following rights:

- Right to be informed (about what data is collected and how it's used)
- Right of access (Subject Access Requests / SARs)
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object (including processing based on legitimate interests or direct marketing)
- Rights relating to automated decision-making and profiling

When personal data is obtained directly from a data subject, the Company shall inform them of the relevant information at the time of collection. Where data is obtained from a third party, the Company shall inform the data subject (where possible) as soon as practicable, and no later than within one month.

Information provided must include: the identity and contact details of the Company (and of the DPO), purposes of processing, legal basis, legitimate interests (if used), categories of personal data, recipients/third parties, details of any transfers outside the UK/EU (with safeguards), retention period, data subject rights, right to withdraw consent, right to lodge complaint with the supervisory authority (the Information Commissioner's Office - ICO), and details of any automated decision-making/profiling.

# 13. Subject Access Requests (SARs) and Responding to Requests

Data subjects may make a Subject Access Request (SAR) at any time to ask what personal data the Company holds about them, why, and how it is used.

The Company's DPO (or designated contact) will handle SARs. The Company will respond within one month of receipt. Where requests are complex or numerous, the period may be extended by up to two additional months - with the data subject informed.

For additional copies of previously supplied information, or for manifestly excessive/repetitive requests, the Company may charge a reasonable fee.

# 14. Rectification, Erasure, Restriction, Portability, and Objection

### Rectification

Data subjects can ask to correct inaccurate or incomplete personal data. The Company will rectify and inform the subject within one month (or up to two months if complex), and inform any third parties to whom the data was disclosed.

### Erasure

Data subjects may request deletion of their personal data if no longer necessary, consent is withdrawn, processing is unlawful, objection is sustained, or legal obligation exists. The Company will erase data unless there are grounds to refuse, and inform data subject (and third parties, where feasible) within one month (or up to two months if complex).

### Restriction

Data subjects may ask to restrict processing. The Company will retain only minimal necessary data and inform relevant third parties of restrictions.

### Portability

Where processing is automated and based on consent or contract, data subject may request a copy of their data in a structured, commonly used, machine-readable format, and (where technically feasible) ask for it to be transmitted directly to another controller. Response within one month (or up to two months if complex).

### Objection

Data subjects may object to processing based on legitimate interest or direct marketing (including profiling). Upon objection, the Company shall cease such processing immediately unless there are overriding legitimate grounds.

# 15. Automated Decision-Making & Profiling

If the Company uses personal data for automated decision-making or profiling (e.g. age-based decisions, attendance-based selection, behavioural profiling, etc), the Company shall:

- Provide clear information to data subjects about the use of profiling / automated decision-making, its significance and likely consequences
- Ensure use of appropriate statistical or mathematical procedures
- Implement technical and organisational measures to minimise risk of errors and allow correction
- Ensure security to prevent discriminatory or harmful effects

Where decisions produce legal or similarly significant effects, data subjects have the right to request human intervention, express their point of view, and obtain an explanation - unless the decision is necessary for contract performance, authorised by law, or based on explicit consent.

# 16. International Data Transfers

Since the UK is outside of the EU, the Company must take care when transferring personal data to countries outside the Uk (or outside the EEA if receiving data from EU).

Transfers must be made only if an adequate level of protection is ensured (e.g. adequacy decision, or appropriate safeguards such as standard contractual clauses, binding corporate rules, or other valid legal mechanisms).

The Company must document all such transfers, and in the case of transfers outside UK/EU, record the safeguards applied, in line with its record-keeping obligations.

# 17. Data Security - Storage, Transfer, Disposal and Use

The Company must ensure:

- Electronic data stored securely (encrypted, access-controlled, properly backed up, offsite where appropriate), with no personal data stored on mobile devices unless authorised, and only for as long as absolutely necessary.
- Hardcopy documents stored securely (locked cabinets, restricted access).
- Secure transmission of data: use secure networks; avoid unsecured/wireless transfers when wired alternatives exist; avoid email with personal data unless encrypted/confidential, and follow internal secure transfer procedures.
- Access control: only authorised staff, agents or contractors who require access for their duties may access personal data.
- No informal sharing or leaving data unattended or on view to unauthorised personnel.

- Strict password policies, regular software updates and patching, prevention of password sharing or insecure handling, and strict control over IT systems.
- Training and awareness for all staff, agents or contractors handling personal data; regular review and audit of data-handling methods and compliance with this Policy.

# 18. Accountability, Training, Supervision and Contractual Controls

- All employees, volunteers, contractors, or other parties working on behalf of the Company who handle personal data must be made aware of their responsibilities under this policy and UK data protection law.
- Only those who need access to personal data for their duties should have access
- All such persons must be contractually bound to comply with this policy and applicable law
- Methods of data collection, holding and processing shall be regularly reviewed and evaluated
- Employee/contractor performance in relation to data protection responsibilities should be assessed
- Periodic reviews, audits, and updates to the policy, data-handling procedures and security measures must be conducted.

# 19. Data Breaches and Notification

- All personal data breaches must be reported immediately to the Company's DPO (or designated responsible person)
- If a breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, reputational damage, discrimination), the Comapny must notify the ICO without undue delay, and in any event within 72 hours of becoming aware of it (where feasible).
- If the breach is likely to result in a high risk to data subjects, the Company must also inform the affected data subjects directly without undue delay
- Breach notifications should include: categories and the approximate number of data subjects affected, categories and approximate number of personal data records concerned, contact details of the DPO, likely consequences of the breach, a description of measures taken or proposed to address and mitigate the breach.

# 20. DEFINITIONS

**The Company** Kanga Sports Ltd, including all employees, workers, contractors, and authorised third parties acting on its behalf

**Personal Data** Any information relating to an identified or identifiable natural person ("data subject"). This includes names, contact details, identification numbers, location data, online identifiers, or any factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of an individual.

**Special Category Personal Data** Personal data requiring additional protection under UK GDPR due to its sensitive nature, including data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic or biometric data (where used for identification)

**Processing / Process** Any operation performed on personal data, whether automated or not. This includes collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, sharing, transmission, restriction, erasure, or destruction

**Data Subject** Any living individual whose personal data is collected, held, or processed by the Company. This may include customers, parents, children, employees, contractors, and third parties

**Data Controller** The organisation that determines the purposes and means of processing personal data. For the purposes of this Policy, the Company is the Data Controller

**Data Processor** Any individual or organisation that processes personal data on behalf of the Data Controller. This may include third-party service providers, platform providers, contractors, or cloud-hosting companies

**UK GDPR** The United Kingdom General Data Protection Regulation, which forms part of UK law following the European Union (Withdrawal) Act 2018

**Data Protection Act 2018 (DPA 2018)** The UK legislation that supplements and clarifies the UK GDPR

**PECR** The Privacy and Electronic Communications Regulations, which govern electronic marketing, cookies, and communications

**Data Protection Officer (DPO)** The individual appointed by the Company to oversee compliance with data protection law and this Policy (where appointed or designated)

**Third Party** Any organisation or individual other than the data subject, the Company, or persons authorised to process personal data under the Company's authority

**Consent** A freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of their personal data

**Personal Data Breach** A security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

**Automated Decision-Making** Decisions made about a data subject solely by automated means, without human involvement

**Profiling** Any automated processing of personal data used to analyse or predict aspects relating to a data subject's behaviour, performance, preferences, or characteristics