

## Active Sport: Data Protection Policy

**Effective Date:** August 2025

**Approved by:** Mark Whitwood (Director)

**Review Date:** August 2026

**Data Protection Lead:** Mark Whitwood (Director)

---

### 1. Purpose

Active Sport Ltd is committed to protecting personal data in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and related legislation. This policy outlines how we collect, process, store, and protect data relating to staff, customers, children, contractors, and other stakeholders.

---

### 2. Scope

This policy applies to:

- All employees, contractors, and volunteers of Active Sport.
  - All personal data processed by Active Sport, whether digital or paper-based.
  - All locations where Active Sport operates.
- 

### 3. Legal Framework

Active Sport complies with the following key legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
  - Data Protection Act 2018
  - Privacy and Electronic Communications Regulations (PECR)
  - Information Commissioner's Office (ICO) guidance
  - Children's Code (for services likely to be accessed by children)
- 

### 4. Data Protection Principles

We adhere to the **7 key principles** of data protection:

1. **Lawfulness, fairness, and transparency**
  2. **Purpose limitation** – only use data for specified, legitimate purposes
  3. **Data minimisation** – only collect necessary data
  4. **Accuracy** – keep personal data accurate and up to date
  5. **Storage limitation** – retain data only as long as necessary
  6. **Integrity and confidentiality** – protect data with appropriate security
  7. **Accountability** – demonstrate compliance with all obligations
- 

### 5. Roles and Responsibilities

Role	Responsibility
<b>Director</b>	Overall accountability for data protection
<b>Data Protection Lead</b>	Oversees compliance, handles Subject Access Requests (SARs), and reports data breaches
<b>All Staff</b>	Must follow this policy and attend annual data protection training

---

### 6. Lawful Bases for Processing

Active Sport processes personal data under one or more of the following lawful bases:

- **Consent** (e.g., marketing communications)
  - **Contractual necessity** (e.g., staff and client agreements)
  - **Legal obligation** (e.g., safeguarding, employment law)
  - **Vital interests** (e.g., medical emergencies involving children)
  - **Legitimate interests** (e.g., improving services, safety management)
- 

### 7. Types of Data We Process

Active Sport may process:

- Contact details (name, address, phone, email)
  - Medical and allergy information (for children's sessions)
  - DBS and safeguarding information (staff and volunteers)
  - Attendance records
  - Payment and invoice data
  - Images and video (with consent)
  - Staff HR records (employment history, training, etc.)
- Sensitive data (Special Category Data) is handled with extra care, using appropriate Article 9 UK GDPR conditions (e.g., explicit consent, safeguarding requirements).
- 

### 8. Data Subjects' Rights

Data subjects have the right to:

- Access their data (Subject Access Request)
- Rectify inaccurate data
- Request data erasure (“right to be forgotten”)
- Restrict or object to processing
- Data portability (where applicable)
- Withdraw consent at any time (where consent is used)

Requests must be addressed to the Data Protection Lead and responded to within **one calendar month**.

---

## 9. Data Sharing and Transfers

- We only share data when legally necessary, with appropriate contracts or safeguards.
  - Data may be shared with: local authorities (e.g., safeguarding), emergency services, HMRC, legal advisors, IT providers, and relevant partners.
  - No personal data is transferred outside the UK without appropriate UK adequacy decisions or standard contractual clauses.
- 

## 10. Data Retention

- We follow a **data retention schedule** based on legal and operational needs.
    - Staff data: 6 months after employment ends
    - Financial records: 6 years (HMRC)
  - Data is securely deleted or anonymised when no longer required.
- 

## 11. Data Security

We implement:

- Password protection and two-factor authentication (2FA)
  - Encryption of sensitive files and backups
  - Limited access rights (role-based)
  - Physical security in offices and storage
  - Regular staff training on data protection
  - Breaches are logged and reported to the ICO within **72 hours** where required.
- 

## 12. Breach Procedure

If a data breach occurs:

1. Notify the Data Protection Lead immediately.
  2. Investigate and assess the risk.
  3. Notify affected individuals if there's a high risk to their rights/freedoms.
  4. Report to the ICO if necessary (via <https://ico.org.uk/for-organisations/report-a-breach/>).
- 

## 13. Children's Data

We follow the **ICO Children's Code**:

- Use clear, age-appropriate language.
  - Seek verifiable parental consent where required.
  - Avoid profiling and behavioural targeting of children.
  - Protect children's rights by default.
- 

## 14. Training and Awareness

- New starters complete induction and read the data protection policy within their first 30 days.
  - Refresher updates are provided following legislative changes.
- 

## 15. Monitoring and Review

This policy will be:

- Reviewed **annually** or when legal requirements change.
  - Updated by the Data Protection Lead and approved by the Director.
- 

## ICO Contact

Information Commissioner's Office

<https://ico.org.uk/global/contact-us/>

---