Premier Rugby Development Ltd

GDPR & Data Protection Policy

1. Policy Statement

Premier Rugby Development is committed to protecting the privacy, confidentiality, and integrity of personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We recognise that personal data must be handled lawfully, fairly, and transparently and that individuals have clear rights regarding how their information is used.

This policy outlines how we collect, process, store, protect, and dispose of personal data.

2. Scope

This policy applies to:

- All employees
- Volunteers
- Directors
- Contractors
- Partner organisations processing data on our behalf

It applies to all personal data processed in both electronic and paper formats.

3. Definitions

Personal Data: Any information relating to an identified or identifiable person.

Special Category Data: Sensitive data including health information, ethnicity, religion, or biometric data.

Processing: Any operation performed on personal data (collection, storage, use, sharing, deletion).

Data Subject: The individual whose data is processed.

Data Controller: Fulfilling Your Potential determines the purpose and means of processing personal data.

Data Processor: A third party processing data on our behalf.

4. Data Protection Principles

We adhere to the seven UK GDPR principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

5. Lawful Bases for Processing

We process personal data under one or more of the following lawful bases:

- Consent
- Performance of a contract
- Legal obligation
- Vital interests
- Legitimate interests

Where Special Category Data is processed (e.g., medical information), we rely on:

- Explicit consent
- Safeguarding of children and adults at risk
- Legal obligations

6. Categories of Data Collected

We may collect and process:

6.1 Participant Data

- Name, date of birth, gender
- Address and contact details
- Parent / carer information
- Emergency contacts
- Medical conditions and allergies
- Attendance and progress records
- Behavioural records
- Safeguarding records

6.2 Staff & Volunteer Data

- Contact details
- Right to work documentation
- DBS information
- Employment records
- Payroll details
- Training records

6.3 Media & Marketing

- Photographs and video recordings (with consent)
- Testimonials

7. How We Collect Data

Data may be collected via:

- Registration forms
- Consent forms
- Online forms
- Email or telephone communication
- Partner referrals
- Direct interactions

We ensure transparency at the point of data collection.

8. Data Use

We use personal data to:

- Deliver programmes and services
- Safeguard participants
- Communicate with parents / carers
- Manage attendance and performance
- Meet legal obligations
- Process payments
- Improve service quality

We do not sell personal data to third parties.

9. Data Sharing

We may share data where necessary with:

- Local Authorities
- Safeguarding agencies
- Police
- Healthcare professionals
- Funding bodies (anonymised where possible)
- IT service providers (under contract)

All third-party processors are subject to data processing agreements.

10. Data Security Measures

We implement appropriate technical and organisational measures including:

- Password-protected systems
- Multi-factor authentication where available
- Encrypted storage
- Secure cloud systems
- Locked filing cabinets for paper records
- Access controls based on role
- Secure disposal (shredding / secure deletion)

Staff receive training on data protection responsibilities.

11. Data Retention

We retain data only as long as necessary for legal, safeguarding, and operational purposes.

Typical retention periods:

- Safeguarding records: In line with statutory guidance
- Staff records: Up to 6 years after employment ends
- Financial records: 6 years
- Registration forms: Duration of involvement + defined retention period

Data is securely destroyed once no longer required.

12. Individual Rights

Individuals have the following rights:

- Right to be informed
- Right of access (Subject Access Request)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making

Subject Access Requests will be responded to within one calendar month.

13. Consent Management

Where consent is relied upon:

- It will be freely given, specific, informed, and unambiguous.
- Written consent will be recorded.
- Individuals may withdraw consent at any time.

14. Data Breach Procedure

A personal data breach is any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

If a breach occurs:

1. It must be reported immediately to senior leadership.
2. The breach will be assessed and contained.
3. A breach log will be completed.
4. The Information Commissioner's Office (ICO) will be notified within 72 hours where required.
5. Affected individuals will be informed where there is high risk.

15. Data Protection Officer (If Applicable)

Where legally required or deemed appropriate, a Data Protection Officer (DPO) will be appointed.

Otherwise, responsibility sits with senior leadership.

16. Privacy Notices

We provide clear privacy notices outlining:

- What data is collected
- Why it is collected
- How it is used
- Who it is shared with
- How long it is retained
- How individuals can exercise their rights

17. International Transfers

We do not transfer personal data outside the UK unless adequate safeguards are in place in accordance with UK GDPR.

18. Monitoring & Compliance

We ensure compliance by:

- Regular policy review
- Staff training
- Data audits where appropriate
- Contract reviews with processors

19. Policy Review

This GDPR & Data Protection Policy will be reviewed annually or sooner if legislation changes.