DATA PROTECTION POLICY

yoursport.org

1. Policy Statement and Commitment

Your Sport Solutions is committed to processing personal data in accordance with the principles of the **General Data Protection Regulation (GDPR)** and the Data Protection Act 2018. This policy sets out the framework and procedures for all staff and volunteers to ensure all personal data is handled lawfully, securely, and transparently.

Our commitment is to protect the rights and privacy of individuals, particularly children and young people, concerning their personal data.

2. Data Protection Principles

All personal data handled by Your Sport Solutions must adhere to the seven core data protection principles:

1. **Lawfulness, Fairness, and Transparency:** Data must be processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimisation:** Data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy:** Data must be accurate and, where necessary, kept up to date.
5. **Storage Limitation:** Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Integrity and Confidentiality (Security):** Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
7. **Accountability:** The data controller (Your Sport Solutions) is responsible for demonstrating compliance with the other six principles.

3. Roles and Responsibilities

Role	Responsibility
Directors	Overall responsibility and accountability for ensuring Your Sport Solutions meets its legal obligations under data protection law.
Data Protection Lead (DPL) / Designated SENDCo	Operational responsibility for overseeing data compliance, managing Subject Access Requests (SARs), handling data breaches, and providing internal guidance/training. Contact: **info@yoursportsolutions.co.uk**.
All Staff and Volunteers	Compliance with this policy and procedures, maintaining data security, reporting any known or suspected data breaches immediately to the DPL.

Export to Sheets

4. Procedures for Data Handling

4.1 Data Collection

- **Consent:** Where consent is the legal basis for processing (e.g., for promotional photos, non-essential communications, or explicit sensitive data processing), it must be **explicit, documented, and easily withdrawn**.
- **Transparency:** Individuals must be clearly informed at the point of collection (via the Privacy Policy) what data is collected, why, how it will be used, and the legal basis for processing.
- **Minimisation:** Only collect data that is strictly necessary for the programme or administrative function.

4.2 Data Storage and Security

- **Digital Data:**
  - All electronic data files containing personal information must be **password protected** and stored on secure, encrypted cloud services or secure company servers.
  - Access to systems containing sensitive data (medical, SEND) must be **restricted** to staff on a strictly need-to-know basis.
  - Staff must use strong, unique passwords and enable two-factor authentication where available.
- **Physical Data (Hard Copies):**
  - Paper records (e.g., printed registration forms, emergency contacts) must be stored in **locked cabinets** or rooms when not in use.
  - Any essential sensitive data taken to a coaching venue must be stored securely during the session and returned immediately after.
  - Physical data must **never** be left unattended or visible in public areas or vehicles.
- **Transmission:** Personal data must not be sent via unencrypted email. Where data must be shared externally, it must be sent securely (e.g., using encrypted files or secure portals).

4.3 Data Retention and Disposal

- Personal data will only be retained for the period specified in the Data Retention Schedule (a document maintained by the DPL).
- Typically, participant records will be retained for a set period (e.g., 6 years after the participant leaves) for legal or insurance purposes.
- Data that has reached the end of its retention period must be **securely disposed of**:
  - **Digital data:** Permanently deleted from all storage locations and backups.
  - **Paper data:** Shredded using a cross-cut shredder or disposed of by a secure destruction service.

5. Data Subject Rights (Handling Requests)

The DPL is responsible for handling all requests from individuals exercising their rights:

- **Right of Access (Subject Access Request - SAR):** Individuals have the right to request a copy of the data we hold about them. Requests must be logged and fulfilled within one calendar month.
- **Right to Rectification:** Requests to correct inaccurate personal data must be actioned immediately.
- **Right to Erasure (Right to be Forgotten):** Requests for data deletion will be actioned unless there is a legal or contractual obligation that requires us to retain the data.

- **Other Rights:** The DPL will also manage requests regarding the rights to restriction of processing, data portability, and objection to processing.

6. Reporting and Managing a Data Breach

A **data breach** is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Immediate Reporting:** Any member of staff or volunteer who suspects or discovers a data breach must immediately notify the **Data Protection Lead (DPL)** via email at **info@yoursportsolutions.co.uk** and/or by phone.
- **Investigation:** The DPL will immediately investigate the breach to determine its scope, cause, and the level of risk to the individuals affected.
- **Regulatory Reporting:** If the breach poses a risk to the rights and freedoms of individuals, the DPL must report the breach to the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of it.
- **Individual Notification:** If the breach poses a high risk to the rights and freedoms of individuals, the DPL will notify the affected individuals without undue delay.

7. Training and Review

All staff and volunteers must undergo regular mandatory data protection and security awareness training. This policy will be reviewed and updated **annually** by the Senior Management team and the DPL to ensure ongoing compliance with evolving data protection legislation.