Data Protection Policy

1. Purpose

This Data Protection Policy outlines how Future Stars Coaching complies with its data protection obligations under UK law. We are committed to safeguarding the privacy of personal data and ensuring all processing is conducted in accordance with applicable laws and best practices.

This policy extends to cover the protection of children's data. Personal data of children, including health information, emergency contact details, and attendance records, will be collected, processed, and stored securely in compliance with the UK GDPR and relevant child protection regulations. We ensure that special measures are taken to safeguard this sensitive data, including obtaining explicit parental or guardian consent for the collection and processing of children's personal data.

2. Scope

This policy applies to all employees, contractors, volunteers, and third-party partners processing personal data on behalf of Future Stars Coaching. It encompasses all personal data collected, stored, and processed through our services, including but not limited to employee, client, and child data. This policy also applies specifically to the processing of personal data relating to children in our care, including health, emergency contacts, and safeguarding records.

3. Definitions

For the purposes of this policy, the following definitions apply:

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

• Processing: Any operation performed on personal data, such as collection, storage, and sharing.

• Data Controller: The organisation responsible for determining the purpose and means of processing.

• Data Processor: Any party processing personal data on behalf of the Data Controller.

Sensitive Personal Data: Special categories of personal data, including but not limited to, health information, racial or ethnic origin, and any data related to a child's physical or mental health or safeguarding status.

4. Data Protection Principles

In accordance with UK GDPR, we adhere to the following principles:

• Lawfulness, fairness, and transparency.

• Purpose limitation: Data will only be collected for specified, explicit purposes.

• Data minimisation: Only the necessary data will be collected.

• Accuracy: Data will be kept accurate and up-to-date.

• Storage limitation: Data will not be stored for longer than necessary.

• Security: Data will be protected against unauthorized access, loss, or damage.

5. Legal Basis for Processing

We process personal data based on one or more of the following legal grounds:

• Consent: Individuals have given clear consent for processing.

• Contract: Processing is necessary to fulfill contractual obligations.

• Legal Obligation: Processing is necessary to comply with legal requirements.

• Legitimate Interests: Processing is necessary for legitimate business interests, unless overridden by the individual's rights.

For the collection, processing, and storage of children's personal data, including health and emergency contact information, explicit consent will be obtained from parents or guardians, in accordance with Article 8 of the UK GDPR. In cases where consent cannot be obtained, processing may be justified based on legitimate interests, such as ensuring a child's safety or well-being. We ensure that consent is freely given, specific, informed, and unambiguous, and that parents/guardians are informed of their right to withdraw consent at any time.

6. Individual Rights

Individuals have the following rights under UK GDPR:

• The right to be informed.

• The right of access.

• The right to rectification.

• The right to erasure (right to be forgotten).

• The right to restrict processing.

• The right to data portability.

• The right to object to processing.

• Rights regarding automated decision-making and profiling.

Parents or guardians may exercise any of the rights outlined above on behalf of their children, including access to, rectification of, or erasure of their child's personal data.

7. Data Security

We implement appropriate technical and organizational measures to protect personal data from unauthorised access, alteration, disclosure, or destruction. This includes:

• Secure storage systems.

• Access controls and encryption.

• Regular security audits and training for employees.

Special care is taken to handle sensitive data, such as medical information (e.g., allergies, special educational needs) that may be necessary for ensuring a child's well-being during our services. Such sensitive data will be processed in compliance with GDPR's additional security measures, including encryption of electronic data, and limited access to ensure only authorized staff members can view this information. Staff members are trained in the handling and confidentiality of this sensitive data.

We regularly review and audit our data security measures to ensure that they remain effective and in compliance with UK GDPR.

8. Data sharing

Children's personal data may be shared with schools, parents, or other relevant external authorities, such as in safeguarding referrals or for the purposes of fulfilling legal or contractual obligations. Any data shared will be done in strict compliance with the data protection laws and safeguarding guidelines, ensuring that only necessary data is shared with appropriate parties and in a manner that upholds confidentiality.

Any data shared with external parties (e.g., schools, safeguarding authorities) will be done so on a need-to-know basis and only for legitimate purposes. We ensure that these third parties adhere to data protection laws and implement appropriate safeguards.

9. Safeguarding Integration

Our data protection procedures are closely linked with our safeguarding policies. Personal data related to children, particularly safeguarding concerns, will be handled with the utmost confidentiality. Personal data related to safeguarding concerns (e.g., reports, health conditions, special needs) will be handled in accordance with the **Children Act 1989** and **Ofsted guidance**. Such data will be stored securely and shared only on a need-to-know basis in line with our safeguarding responsibilities.

10. Data Retention for Records

Children's/parent's/guardians'/employee's personal data, including attendance records, health information, and safeguarding records, will be retained only for as long as necessary to fulfil the purpose for which it was collected. We retain such data in line with legal requirements, including guidance from Ofsted and child protection laws. After the retention period, data will be securely deleted or anonymised. Where possible, we will align our retention practices with the specific requirements of our services and statutory bodies.

Children's personal data will be retained in line with statutory retention periods, such as those set out in Ofsted guidance. Where no statutory period is provided, data will be kept only for as long as is necessary for the purposes for which it was collected and processed.

11. Data Breaches

In the event of a data breach, we will follow the procedures outlined in our Data Breach Response Plan, which includes notifying the Information Commissioner's Office (ICO) and affected individuals as required.

In the event of a data breach involving children's personal data, we will follow the procedures outlined in our breach response plan. This includes notifying affected parents or guardians, as well as the Information Commissioner's Office (ICO), within the required 72-hour timeframe when applicable. We will assess the breach to determine whether it poses a risk to the rights and freedoms of the child and take appropriate actions to mitigate any harm caused.

In the event of a data breach involving sensitive data, we will assess whether the breach could result in significant harm to the individuals concerned, including children, and will take appropriate steps to

mitigate any risks. We will notify the ICO and affected individuals, including parents or guardians, if required.

12. Third-Party Processing

When personal data is shared with third parties for processing, we ensure they comply with data protection laws and implement safeguards to protect the data.

13. Employee Training

All employees receive regular training on data protection and are required to adhere to this policy. Training will be organised by the Data Protection Officer (DPO) and is mandatory for all staff handling children's data. Training will be reviewed and updated annually, with refresher courses as needed.

All staff members who handle personal data will receive regular training on the importance of confidentiality, secure data handling, and safeguarding procedures. This training is mandatory and includes specific guidance on the protection of children's data, with a focus on ensuring that sensitive information is securely stored and only accessed by authorized personnel. The training program will be reviewed annually.

14. Policy Review

This policy will be reviewed annually or in response to significant changes in the law, business practices, or technological advances, ensuring ongoing compliance with data protection laws.