FUTURE SUCCESS SPORTS PRIVACY & DATA PROTECTION (GDPR) POLICY

Introduction

Future Success Sports is committed to protecting personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

Data Handling

- Lawful collection and processing of personal data.
- Secure storage and restricted access to personal information, with access limited to authorized personnel only. All personal data will be stored in encrypted digital systems and locked physical storage where applicable, ensuring compliance with UK GDPR. Regular audits will be conducted to review data security measures, and any breaches will be reported in line with ICO regulations and FA safeguarding standards.
- Clear communication on how data is used, including the purposes of data collection, who it will be shared with, and how long it will be retained. Individuals will have the right to withdraw consent at any time, and procedures for doing so will be clearly outlined in sign-up documentation and privacy notices.
- Personal data will be retained only for as long as necessary to fulfil its intended purpose, in compliance with UK GDPR and FA safeguarding standards. Standard retention periods will be clearly outlined in our data retention policy, after which data will be securely deleted or anonymized. Any data required for safeguarding purposes will be stored in line with FA requirements and statutory obligations.
- Parental consent obtained for data collection related to children under 18.

Data Breach Reporting and Rectification Procedures:

- **Immediate Containment:** Any suspected or confirmed data breach must be reported immediately to the company directors, who will act as Data Protection Officers (DPOs) and initiate an immediate risk assessment.
- **Assessment & Investigation:** The DPOs will assess the scope and impact of the breach, determine what data has been compromised, and take necessary steps to contain it.
- **Notification & Reporting:** If the breach poses a risk to individuals' rights and freedoms, it will be reported to the Information Commissioner's Office (ICO) within 72 hours, in compliance with UK GDPR. Affected individuals will also be informed if there is a high risk to their data security.
- **Remedial Action:** Steps will be taken to rectify the breach, such as strengthening security measures, reviewing policies, and implementing additional staff training where necessary.
- **Documentation & Review:** All breaches will be recorded, including the nature of the breach, actions taken, and lessons learned. An internal review will be conducted to prevent future occurrences, with necessary updates made to data protection policies and procedures.
- **Compliance with FA Safeguarding Standards:** Where data breaches involve safeguarding-related information, The FA's Designated Safeguarding Officer (DSO) will be notified as per regulatory

requirements.
- Compliance with FA safeguarding standards for data handling.

Implementation

- Staff training on GDPR compliance.
- Secure digital and physical storage systems.
- Clear policies on data sharing and retention periods.
- Data Breach Procedure in place to handle security incidents via class for kids software.
- Regular compliance audits to ensure adherence to regulations.
- Escalation of data protection breaches to the Information Commissioner's Office (ICO) where necessary.

Review and Updates:

This policy will be reviewed annually by the company directors to ensure compliance with UK regulations and FA guidelines. The review process will include assessing updates to relevant legislation, FA policies, and best practices, as well as feedback from staff and stakeholders.

This policy is effective as of 27th January 2025.