Sutton United Football Club – Data Protection Policy

1. Purpose

This policy outlines how Sutton United Football Club collects, uses, stores, and protects personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Scope

This policy applies to all club officials, volunteers, coaches, and anyone else who handles personal data on behalf of the club.

3. Key Definitions

- Personal Data: Information that identifies an individual (e.g. name, address, email, contact number, next of kin/parent/guardian).
- Special Category Data: Sensitive data such as health information or ethnicity.
- Data Subject: The individual whose data is being processed.
- Controller: The club, which decides how and why personal data is used.
- Processor: Any third party who processes data on behalf of the club (e.g. a registration platform).

4. Club Personnel General Obligations

- All Club personnel must comply with this Policy.
- Club personnel must ensure that they keep confidential all personal data that they collect, store, use and come into contact with during the performance of their duties.
- Club personnel must not release or disclose any personal data:
    - outside the Club
    - inside the Club, to Club personnel not authorised to access the personal data

Without specific authorisation from the Data Protection Lead.

- Club personnel must not misuse personal data.
- Club personnel must take all steps to ensure there is no unauthorised access to, or authorised access misuse of personal data whether by Club personnel who are not authorised to see such personal data or by people outside the Club.

5. Principles of Data Protection

When using personal data, the Club will comply with the following data protection laws including the following principles:

- Lawfulness, fairness, and transparency.
- Purpose limitation - for specific, legitimate purposes.
- Data minimisation – only what is necessary.
- Accuracy - kept up to date and accurate.
- Storage limitation – kept for no longer than necessary.
- Integrity and confidentiality – kept securely protecting against loss, misuse, or unauthorised access.

- Accountability – demonstrate compliance with GDPR principles

6. Lawful Basis for Processing

The Club will only collect and use personal data when we have a lawful reason to do so under Article 6 of the UK GDPR, such as:
- Consent from the individual.
- Performance of a contract (e.g. player registration).
- Legal obligation (e.g. safeguarding).
- Legitimate interests (e.g. club communications).

When the Club collects and/or uses Special Categories of personal data, the Club has to show that one of a number of additional conditions is met under Article 9 of the UK GDPR. Detailed additional conditions are found at Special category data | ICO.

7. Privacy Notices

The Club will inform individuals how their data is used via a privacy notice available on the Club website or during registration.

8. Data Security

The Club will take reasonable steps to protect personal data, including:
- Encrypted systems.
- Limited access to data.
- Secure disposal of paper records.

9. Data Retention

Data Protection Laws require that the Club does not keep personal data longer than is necessary for the purpose or purposes for which the Club collected it, typically 6 years after completion of the programme/membership, unless otherwise legally required.

10. Individual Rights

UK GDPR gives data subjects more control about how their data is collected, stored and what is done with it.

The different types of rights of data subjects are:

- Access the personal data we hold about you (Access)
- Request correction of inaccurate or incomplete data (Rectification)
- Request erasure of records or withdraw consent (Erasure: 'right to be forgotten')
- Object to or restrict processing in certain circumstances (To object)
- Transfer of data from one controller to another (Data Portability)
- Not to be subject to automated decision-making including profiling – the Club does not use automated decision-making

The Club will use all personal data in accordance with the rights given to data subjects under Data Protection Laws, and will ensure that it allows individuals to exercise their rights.

Individual Rights Requests should be sent to the Data Protection Lead.

11. Data Breaches

There are three main types of personal data breach which are as follows:
- **Confidentiality breach**: Occurs when personal data is disclosed, accessed, or misused without authorisation—examples include hacking, unauthorised access to internal systems, sending data to the wrong person, or losing a device containing personal data.
- **Availability breach**: Involves the loss of access to or destruction of personal data—such as through ransomware, accidental deletion, lost devices, or failure to restore data from backups.
- **Integrity breach**: Happens when personal data is altered without authorisation or by accident.

Any suspected near miss or data breach must be reported immediately to the Data Protection Lead, (academy@suttonunitedfc.co.uk, Phone: 07591170639).

Serious breaches may be reported to the ICO.

12. Third Parties

We will ensure any third-party services (e.g. online registration platforms) comply with data protection laws and have appropriate agreements in place.

13. Transfers Outside the UK

We will not transfer personal data outside the UK unless adequate safeguards are in place and approved by the Club Committee.

14. Complaints

Any complaints about the use of personal data should be directed to the Data Protection Lead who will acknowledge within 30 days and respond without undue delay.