Data Protection Policy

Introduction

Sporting Communities collects and processes information about individuals including service users, employees, volunteers, suppliers, and business contacts. This policy outlines how personal data must be collected, handled, and stored to comply with UK data protection laws, including the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

This policy ensures that Sporting Communities:

- Complies with all relevant data protection laws and best practices.
- Protects the rights of individuals, ensuring privacy and security.
- Is transparent about how personal data is managed.
- Safeguards the organisation from the risk of data breaches.

Why This Policy Exists

This policy aims to:

- Ensure compliance with data protection law and best practices.
- Protect the rights and privacy of employees, volunteers, service users, and stakeholders.
- Ensure transparency in the way personal data is stored, processed, and used.
- Protect Sporting Communities from data breaches and the associated risks, including legal penalties and reputational damage.

Data Protection Law

Sporting Communities must handle personal data in line with the Data Protection Act 2018 and GDPR. This applies to all personal information, whether stored electronically, on paper, or on other materials.

Under the law, personal data must be:

- Processed lawfully, fairly, and transparently.
- Collected for specific, legitimate purposes and not used for other purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Stored only as long as necessary.
- Processed in a way that ensures security and confidentiality.

Records will be destroyed when no longer needed, except for safeguarding, legal, or welfare reasons. These records will be kept for a period of seven years, or for children, until they turn 25 (seven years after reaching school-leaving age).

Scope of the Policy

This policy applies to all staff, volunteers, and contractors working with or for Sporting Communities. It covers all personal data, including but not limited to:

- Names, addresses, phone numbers, and email addresses.
- Any other data relating to identifiable individuals.

Data Protection Risks

This policy helps protect Sporting Communities from:

- Breaches of confidentiality.
- Failing to give individuals control over their personal data.
- Damage to the organisation's reputation due to mishandling personal data.

Responsibilities

Everyone involved with Sporting Communities is responsible for ensuring compliance with this policy. Specific responsibilities include:

- **Board of Directors**: Ultimately responsible for ensuring legal obligations are met.
- **Chief Executive Officer (CEO)**:
  - Keeps the board informed of data protection responsibilities, risks, and issues.
  - Ensures that data protection procedures and policies are reviewed regularly.
  - Arranges for data protection training and advice for staff and volunteers.
  - Handles requests for access to personal data (Subject Access Requests).
  - Ensures contracts with third parties handling personal data meet GDPR requirements.
- **Managing Director**:
  - Ensures all data storage systems meet security standards.
  - Performs regular checks on data security measures.
  - Evaluates third-party data storage services (e.g., cloud services).

    - Oversees the organisation's response to data protection queries from the public or media.

General Guidelines for Staff and Volunteers

- Only individuals who need access to data for their work should have it.
- Data must not be shared informally and should be accessed through appropriate channels.
- Employees must follow all data protection training and guidelines.
- Strong passwords (8+ characters, including numbers and symbols) must be used and updated regularly.
- Personal data should never be shared with unauthorised individuals.
- Outdated or inaccurate data must be updated or deleted.
- Any concerns about data protection should be raised with the line manager or the Data Protection Officer.

Data Storage

Data must be securely stored, whether in electronic or physical format:

- **Paper Records**: Must be stored in locked drawers or cabinets when not in use. Printed data should not be left unattended, and must be shredded when no longer required.
- **Electronic Data**:
    - Strong passwords must be used, and data should only be stored on approved servers or cloud platforms.
    - Data must not be saved on portable devices like laptops, phones, or tablets unless encrypted.
    - Regular backups of electronic data must be performed and securely stored.
    - All devices storing personal data must be protected by approved security software and firewalls.

Data Use

Personal data should only be used for the purposes for which it was collected. When using personal data:

- Employees must ensure that computer screens are locked when unattended.
- Personal data should not be shared informally or through unsecured methods such as email.
- Employees should avoid storing copies of personal data on personal devices; all data should remain in centralised systems.

Data Accuracy

Sporting Communities is required to take reasonable steps to ensure that personal data is accurate and up to date:

- Data should be updated as necessary, and inaccurate information should be corrected or deleted promptly.
- Staff must regularly check and update records, particularly when receiving new information from service users or stakeholders.

Individual Rights

Under **GDPR**, individuals have the following rights:

- **The right to be informed**: Individuals will be informed of how their data is collected, stored, and used through privacy notices.
- **The right of access**: Individuals can request access to their personal data through a Subject Access Request. These requests must be submitted in writing and will be responded to within one month.
- **The right to rectification or erasure**: Individuals can request that inaccurate data be corrected or that their personal data be erased.
- **The right to restrict processing**: Individuals can request limitations on how their data is processed.
- **The right to object**: Individuals can object to their data being processed, especially for direct marketing purposes.

Accountability

Sporting Communities is committed to being accountable for data protection compliance by:

- Regularly reviewing and updating data protection policies and procedures.
- Taking a "data protection by design and default" approach to ensure data protection is embedded in all activities.
- Maintaining up-to-date documentation of all data processing activities.
- Implementing security measures and reporting any data breaches to the Information Commissioner's Office (ICO) where necessary.
- Training all staff and volunteers on data protection responsibilities.

Subject Access Requests

All individuals have the right to know what data is held about them and how it is processed. Subject Access Requests should be made in writing and addressed to the Data Protection Officer at info@sportingcommunities.co.uk The organisation will respond within one month. Verification of identity may be required before processing the request.

Disclosing Data

In certain circumstances, personal data may need to be disclosed to law enforcement or regulatory agencies without the consent of the individual, as required by law. The Data Protection Officer will ensure that any such disclosure is legitimate and compliant with legal requirements.

Providing Information

Sporting Communities will ensure that all individuals are informed about how their data is processed and how they can exercise their rights.

The Data Protection Officer (DPO) for Sporting Communities is Ben Rigby (Managing Director).
Contact details:

- **Email**: info@sportingcommunities.co.uk
- **Phone**: 07966 984147