Sporting Communities CIC
Data Protection Policy

Introduction

Sporting Communities needs to gather and use certain information about individuals. These can include service users, customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law. Sporting Communities adheres to the guidelines of the Data Protection Act 1998, the Data Protection Act 2018 and Article 5 of the General Data Protection Regulation (GDPR).

Why this policy exists

This data protection policy ensure that Sporting Communities:

- Complies with data protection law and follow good practice
- Protects the rights of workers, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

Sporting Communities must collect, handle and store personal information in line with the Data Protection Act 1998, Data Protection Act 2018 and Article 5 of the General Data Protection Regulation (GDPR).

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Legislation requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. 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; and
6. 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. Records of personal information will be destroyed when participants no longer utilise the service, or when workers / volunteers no longer work / volunteer for the company.
8. An exception to this is if data is required for safeguarding, incidents, welfare or legal requirements
9. Safeguarding, incidents, welfare or legal records will be kept for a 7 year period, or in relation to children, until the child is 25 (this is seven years after they reach the school leaving age).

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

Policy scope

This policy applies to all who work and volunteer for or with Sporting Communities.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

Data protection risks

This policy helps to protect Sporting Communities from some very real data security risks, including:

- Breaches of confidentiality
- Failing to offer choice
- Reputational damage

Responsibilities

Everyone who works for or with Sporting Communities has some responsibility for ensuring data is collected, stored and handled appropriately. Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles, however, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Sporting Communities meets its legal obligations.
- The Chief Executive Officer is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from workers and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Sporting Communities holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The Managing Director, is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other workers to ensure marketing initiatives abide by data protection principles.

General workers guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Sporting Communities will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, strong, complex passwords of at least 12 characters, mixed of upper and lower case letters, numbers and symbols.
- Passwords must be used and they should never be shared.
- Passwords should be unique and not repeated
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Administrator.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Sporting Communities, other than for statistical monitoring and reporting, or in sensitive cases, where information is required to be shared for the safeguarding of the service user.

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy
The law requires Sporting Communities to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Sporting Communities should put into ensuring its accuracy.
It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Hard copies of data are to be held in a central locked location. Workers should not create any unnecessary additional data sets.
- Workers should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Individual & Other Rights
Sporting Communities will adhere to the GDPR rights for individuals (incl. member representatives) which stipulate:

- The ***right to be informed*** about the collection and use of their personal data. Sporting Communities will provide individuals/member organisations with privacy information including the purposes for processing their personal data, our retention periods for that data and who it will be shared with.
- The ***right to access*** their personal data and supplementary information so they can be aware of and verify the lawfulness of the processing. To submit a subject access request the individual/member should apply in writing detailing the information they require access to, this should then be sent to the Data Protection Officer. In some cases Sporting Communities may need to ask for proof of identity before processing the request, if this is the case we will inform the individual which documents we require.
- Sporting Communities will respond to a request within one month from the date of receipt and this will normally be in an electronic format, unless requested otherwise. If a subject access request is manifestly unfounded or excessive the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee based upon the administrative cost of responding to the request.
- The ***right to rectification or erasure*** allows individuals to request that any inaccurate personal data is rectified/updated or that their data is permanently erased. A request for rectification or erasure should be made in writing to the Sporting Communities Data Protection Officer who will

complete the request within one month from the date of receipt. Electronically held data will be irretrievably deleted, hardcopy data will be shredded and disposed of securely.

- The ***right to restrict processing*** enables individuals to restrict or stop how their data is being processed whereby it's no longer necessary for the purposes of the processing; if the individual's rights override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data) or if there is a dispute relating to this override of individuals rights.
- The ***right to object*** to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling) and direct marketing (including profiling). Individuals can also complain to the Information Commissioner if they think Sporting Communities has failed to comply with data protection legislation.

Accountability

Sporting Communities take responsibility for complying with the GDPR, at the highest management level and throughout our organisation. We will keep evidence of the steps we take to comply with the GDPR and will put in place appropriate technical and organisational measures to safeguard personal information. This will include:

- Adopting, implementing and reviewing our data protection policy and underpinning policies on a regular basis
- Taking a 'data protection by design and default' approach - to ensure data protection measures are in place throughout the lifecycle of our processing operations;
- Securing confirmation of satisfactory safeguards being in place with organisations that process personal data on our behalf;
- Maintaining documentation of our processing activities;
- Implementing appropriate security measures and recording/reporting personal data breaches;
- Ensuring data protection safeguards are an integral part of our risk assessment processes

Subject access requests

All individuals who are the subject of personal data held by Sporting Communities are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to admin@sportingcommunitiescic.org. A standard request form can be supplied, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The relevant data will then be provided within 14 days.

The Managing Director will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Sporting Communities will disclose requested data, however, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Sporting Communities aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

Sporting Communities' has a designated Data Protection Officer. The key responsibilities of the Data Protection Officer are to:
Oversee changes to systems and processes;
Monitor compliance with the GDPR;

- Report on data protection and compliance with legislation to trustees;
- Liaise, if required, with the Information Commissioner's Office (ICO).

Data Protection Impact Assessment

The Data Protection Officer is responsible for regularly undertaking a thorough Data Protection Impact Assessment in line with ICO guidance.