Portsmouth Joggers Club

Data Protection Policy

Policy Statement

Portsmouth Joggers Club is committed to protecting any personal data it is entrusted with. The data kept by the Club should not extend beyond what is reasonably required to meet the administrative needs of the club.

All members of the club who have access to the personal data held by the club are expected to have read and to abide by this policy. The constitution of the club outlines disciplinary procedures that may be enacted upon anyone found to have acted without due regard to this policy.

Legal Status

Portsmouth Joggers Club is a small not-for-profit organisation where data collection and storage is limited to the membership database. Under current law the Club is exempt from mandatory registration under the Data Protection Act but has chosen to register with the Information Commissioner's Office.

Security of Data

This policy requires that any personal data held by the club be securely kept and that reasonable steps be taken to ensure it remains confidential.

a) Access to the data is only granted where it is appropriate for the administrative needs of the club.

b) Stored electronic data should be appropriately encrypted when not in active use or during transportation.

c) Redundant or transient copies of data should be safely disposed of when no longer required (i.e. membership renewal forms should be shredded). This applies to both physical and electronic copies.

Stored Data

Scoped Data (Data this Policy Applies to)

a) Membership Database: The Club maintains a database of its members. This includes basic personal information required for the administration of the club such as identification, contact details, payment status, date of birth and optional UKA affiliation data.

b) Any addition to the scoped data collected or processed by the club would be regarded as a substantial change and would require re-evaluation of this policy document.

Out of Scope (Data this policy does not apply to)

a) UK Athletics: Club members have the option of UKA affiliation when they join or renew their membership. By necessity affiliation requires passing on a subset of the data held for those members who have opted into this. The data concerned passes beyond the control of the Club, members should consult UKA documentation for that organisations policies and operating procedures.

b) Social Media: Club members may optionally have signed up independently to groups on social media sites that reference the club name (Such as Facebook, Strava, Runkeeper etcetera). These services operate independently under their own data policies. Concerned members should check the policies of those services independently.

c) Race Signup: Signups to races and events (organised by the club but open to non-members, organised by affiliates of the club or organised by 3rd parties but mentioned at a club night) operate separately. Data policy information should be available at time of signup.

d) CCTV: The club does not own or operate CCTV systems, members attending club events however should be aware that venues the club uses may operate CCTV systems (Including 1000 Lakeside) that will be covered under the venues own data protection policies.

Disclosure of Data

Personal data entrusted to the club should only be used for proper administration of the club. Transfer of the data would be regarded as appropriate only in the following circumstances:

a) A court order, a request by a law enforcement agency or any other circumstance where such disclosure is required to comply with the law.

b) Where data is transferred to a person within the club engaged in an administrative role where access to the data is prerequisite. This should only take place with if the person confirms they have read, understood and accept the responsibilities present in this policy document.

c) A third party organisation who is to perform services or administration on behalf of the club (Such as Insurance, membership payment or other service where there is a clear benefit to the club and it's members). This should only take place with the agreement of the committee after appropriate due diligence has established that the reputation and policies of that organisation are compatible with the stated goals of this policy document.

Notification of Breach

If the committee becomes aware of a breach, steps should be taken to immediately correct the breach. Anyone whose data is affected should be notified at the earliest opportunity.

The committee should investigate if the breach was as a result of a failure to comply with this policy. In the case of a severe breach the Data Protection Officer should be prepared to make a full report at the next AGM or EGM, this should include extent of breach, exploration of cause, recommendations for remedial action and any amendments necessary to policy.

Responsibilities

The committee is the data controller under the Act

A data protection Officer has been appointed who is responsible for day-to-day data protection matters and for maintaining policy for the club.

Members of the Club are responsible for ensuring that their personal data supplied to this club is accurate and up-to-date.

Right of Access to Data (Subject Access Request)

Any person whose data is held by the Club has a right to access the data held to confirm its accuracy. Members wishing to check their data should contact the membership secretary (membership@pjc.org.uk) from their recorded email address. If there is no email address on file, or that address has changed contact the membership secretary or a committee member on a club night.

References

http://pjc.org.uk/ (Portsmouth Joggers Club)

http://www.englandathletics.org/ (UKA)

https://www.gov.uk/data-protection/the-data-protection-act (Data protection Act Notes)

https://ico.org.uk/ (The Information Commissioner's Office)