

# Data Protection Policy



## INTRODUCTION

In order to function as a cycling club under its current constitution and rules the club has to ask for and store data on its members and others. This data may include:

- Membership lists
- Member contact details including email
- Photos of members and others
- Sign on sheets
- Race and event participation records
- Financial records
- Records for the purpose of sporting body and Government regulation compliance
- Other purposes necessitated by the act of running the club as constituted

The club will ensure that all data is held and processed in accordance with the requirements of current data protection legislation including General Data Protection Regulation (“GDPR”).

The club approach to GDPR will be kept under constant review to ensure that it remains compliant as GDPR evolves. Accordingly, the Club Committee Meetings will have Data Protection as a standing item to ensure it is aware of new developments regarding data safeguarding and practice, so ensuring that the club is compliant with its obligations.

## RATIONALE FOR DATA PROCESSING

In general, the club processes information under its “Legitimate Interests” and / or with the consent of its members. (The club has a legitimate interest in processing data where there is a relevant and appropriate relationship between the data subject and the data holder).

However, consent is required for such normal activities as being mentioned in an event write-up that may not be viewed (legally) as intrinsic to the club function. The club Data Controller is Paul Haig he may be contacted at the following email address [sikhcyclingclub@hotmail.com](mailto:sikhcyclingclub@hotmail.com) or failing this the Chair of the club shall assume responsibility.

The responsibilities of the Data Controller are:

- a) Responding to information requests (members, former members or third parties). These should be sent to the Data Controller who is then responsible for ensuring that they are processed and responded to within the guidelines set out by GDPR.
- b) Determining whether the request is legitimate, whether it is something which the club needs to respond to, and for determining what information is held by the club on that individual (through liaison with the appropriate members of the club).
- c) Ensuring all information is destroyed at the appropriate point in accordance with the

# Data Protection Policy



requirements of GDPR (and HMRC where relevant). In general, the following deadlines shall apply to the destruction of data:

- Member contact details; one year after termination of membership
- Accounts 6 years following last financial year
- Compliance records two years after period referenced
- Cycling performance records: only on request of record holder

The data destruction policy shall be kept under review by the Data Controller in conjunction with the Club Committee to ensure it remains compliant as GDPR evolves.

The data held is for the purpose of running the club as it has historically operated. Data will not be released to any third party of a different generic type to those that have formally received such information.

Typical previous recipients have included:

- Government
- Sporting Bodies
- Local media in respect of time trial results etc

Participation data required to evidence CASC compliance to HMRC will be kept for 7 years.

Other data will not be stored for more than two years after a member has ceased membership or will be destroyed on request to the Data Controller.

All data will generally be stored digitally, and password protected where practical. Personal Data will not be transferred outside the EU.

Non-Electronic records will also be retained securely where they are used and subject to the same controls as electronic records. Destruction of these records types (generally paper) will be by complete destruction i.e. either shredding or burning.

Personal information held at home by club officials needs to be secured as would their own personal information.

Data will not be used for profiling as defined in law.

All data subjects (you) have the right to withdraw consent; please contact the Data Controller in the first instance.

All data subjects have the right to complain to the Supervisory Authority (the Information Commissioner's Office ("ICO"))

# Data Protection Policy



**THE CLUB IS UNABLE TO ACCEPT MEMBERS WHO ARE UNWILLING TO AGREE TO THEIR DATA BEING PROCESSED UNDER THE ABOVE POLICY.**

## **RIGHT TO ERASURE**

The club will comply fully with Article 17 of GDPR on the “right to erasure” (right to be forgotten).

The club shall erase personal data without undue delay where one of the following grounds applies:

- a) The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed
- b) The data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing of the data
- c) The personal data have been unlawfully processed
- d) The personal data will be erased for compliance with a legal obligations that are applicable in the UK.
- e) If a “Right to Erasure” is agreed by the GDPR Administrator that does not meet the above then the individual requesting that “right to erasure” will no longer be a member of A5CC and no refund on their membership will be granted.

## **NOTIFICATION OF A BREACH**

The club takes its responsibility to manage the data it holds seriously, and shall notify the ICO within the required timescales of any breach which falls within the obligation to notify the Authority.

Upon discovery of a breach, the Data Controller shall inform the ICO without undue delay, and certainly not later than 72 hours after discovery.

In accordance with the provisions of GDPR, where a data breach is likely to be a high risk to the rights and freedoms of individuals the Data Controller shall ensure that the club communicates the nature of the breach, in plain English, to the data subjects concerned, without undue delay.

The club shall not notify the data subject where the breach falls under the following criteria:

- a) Where the club has implemented protection measures in respect to the personal data affected by the breach (e.g. the data was encrypted)
- b) Where the club has taken subsequent measures to ensure that high risk to the rights and freedoms of the individual is no longer likely to arise.

## **Image Permission:**

SCC takes and uses photographs for the purpose of recording, publicising and celebrating participation and achievement of our members in coaching sessions, club rides, time trials, races and other events. These images may be shared with local and national media and on social media if appropriate. Members are assumed to give permission for these images to be used in this way but may opt out on request at the point of joining or renewing membership.

# Data Protection Policy



Updated 01/12/2025