

Data Protection Requirements for SCA Event Organisers and Affiliated Club Membership Secretaries

This guidance applies to:

- Club Membership Secretaries of all clubs affiliated to SCA
- Event organisers within SCA Affiliated Clubs organising SCA events

1. Introduction

As individuals, we want to know that personal information about ourselves is handled properly, and we and others have specific rights in this regard.

Whether we are organising an SCA event or managing the membership records of a club, we need to collect, store and process personal information. It is recognised that the correct and lawful treatment of this information will maintain confidence in the organisation and will maintain the security and privacy of such information.

Personal information, which is not limited to that stored electronically, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how organisations (including the SCA and Affiliated Clubs) may process personal information. A breach of the Act could give rise to criminal and civil sanctions as well as bad publicity.

2. SCA Data Protection Policy

Club Membership Secretaries and organisers of SCA events should be familiar with the SCA Data Protection Policy (and/or their club's own equivalent policy), which sets out the key responsibilities under the Data Protection Act 1998 and the SCA procedure for meeting the requirements of the legislation. The SCA Policy is available on the website at: www.canoescotland.org/about in the section labelled SCA Policies and Documents. When collecting data from individuals, reference should always be made to the SCA Fair Processing Statement (available from www.canoescotland.org/join-us/membership). This statement outlines what the SCA will do with the data. Template statements are also available for clubs to use when managing membership records and when organising events.

Maintaining the security of data

(a) Paper or other physical records e.g. event entry cards, membership forms etc.

- Entry cards, membership forms etc. should be kept securely when not being processed or accessed.
- Ensure that only those legitimately requiring access to personal data are permitted access.

(b) Electronic records e.g. spreadsheets on a computer

If you are using a computer and software to process or record personal data:

- Ensure the computer/device has up to date anti-virus programmes installed and operating.
- Password protect the computer/device so that only an authorised user can gain access. If it is a shared computer/device, ensure that individual logins are used to prevent unauthorised people gaining access.
- Lock the computer/device screen to prevent unauthorised access when unattended.

- Ideally computer/device hard drives should be encrypted. Computers/devices should not be left unattended and ideally will be physically secured to an immovable object to prevent them being removed by an unauthorised person.

3. Considerations when using email and when publishing data (e.g. results, trip reports, trip calendar, organiser details etc.)

It is very easy to send or publish more information than intended or needed particularly where e.g. spreadsheets contain personal data that should not be published in e.g. results sheets.

- Consider using the bcc (blind carbon copy) feature if sending an email to a group of people rather than displaying recipient email addresses.
- Consider how much information the recipient requires and reduce the information included to just what is necessary.
- Be careful not to transmit data in e.g. spreadsheet cells that are hidden or data that is in a separate worksheet within a spreadsheet.
- Best practice is to produce a pdf of the information for email and websites rather than using a spreadsheet.
- Always check what data you have included before sending an email or publishing information on a website.

4. Retention and disposal (e.g. after an event or at the end of a club membership)

The Data Processor's responsibility regarding Data Protection does not end when the event finishes or the individual leaves membership of the club. They are responsible for secure handling/transfer/disposal of all data collected through the organisation of the event/management of membership. Points to consider:

- If you organise a British Canoeing ranked competition there will be specific processes to be followed set out by the relevant British and/or Scottish competition discipline committee regarding results, rankings, promotions, demotions etc.
- If the event is a standalone SCA Event, there will be information to pass back to the SCA office.
- If the data relates to a membership and the member leaves the club, consider how long it is necessary to retain their details. The Data Protection Principles from the act stipulate that data should not be kept for longer than necessary.
- In the case of events, there may be Day Membership forms to return to the SCA Office.

Regardless of which type of event you organise, you are responsible for ensuring that the physical records that exist after an event are returned to the designated person - or if some physical records are not required to be returned that they are securely disposed of e.g. shredded.

The same applies to electronic/computer records. After the necessary information has been transferred to e.g. results compilers, ranking list officers, SCA administrators etc. all electronic records should be deleted from computers/devices ensuring that records do not remain in "trash", "recycle bin" etc.

5. Further Information and Advice

It is recognised that people volunteer to run events because of their love for our sport and not because of desire to be a "Data Processor" as defined under the Data Protection Act.

If you have any questions about Data Protection and how it applies to running SCA events please contact the SCA Data Controller: stuart.smith@canoescotland.org