SCA Data Protection Policy

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. In the course of its activities, the Scottish Canoe Association (SCA) will collect, store and process personal information, and it recognises that the correct and lawful treatment of this information will maintain confidence in the organisation and will provide for successful operations.

The types of personal information that SCA may be required to handle include information about:

- members (of both SCA, affiliated clubs and approved centres) and, where applicable, their guardians;
- current, past and prospective employees, officers, board and committee members, volunteers, SCA representatives, advisers, consultants, contractors and agents;
- registered athletes being individuals who are members of National Programmes who compete and represent Scotland at a national level;
- those individuals who have undertaken training or qualifications through SCA or partner organisations;
- coaches and course providers registered with the SCA;
- suppliers and sponsors;

and others with whom it communicates.

The personal information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards.

2. Status of the Policy

This policy sets out the SCA's policy on data protection and specifies how the SCA will comply with the current legislation regarding the receiving, storage, processing, retention and disposal of personal information.

This policy applies to all those who process data within the SCA. For employees it is a condition of employment.

Any breach of the policy will be taken seriously and may result in disciplinary action. Negligent or deliberate breaches could also result in personal criminal liability.

Any employee, board or committee member, volunteer, SCA representative, adviser, consultant, contractor or agent who considers that the policy has not been followed in respect of personal information about themselves or others should raise the matter with the SCA Data Protection Officer in the first instance.

3. The meaning of Data Protection Terms

Personal data means any information relating to an identified or identifiable natural person (a data **subject)**

- **For example, name, address, date of birth or email address of members, athletes, coaches, participants, employees, volunteers or parents**

Processing means any operation performed on personal data (including automated operations), including collecting, storing, consulting, using, disclosing, amending, deleting, etc.

- **For example, asking individuals to complete a form online, inputting their information into a database, sending communications, etc.**

Special categories of personal data means data revealing a **natural person's:**

- **Racial or ethnic origin**
- **Political opinions, religious or philosophical beliefs**
- **Trade union membership**
- **Genetic or biometric data for the pu**rpose of uniquely identifying a **natural person**
- **Data concerning health**
- **Data concerning a natural person's sex life or sexual orientation**

Controller means the person who determines the purposes and **means of processing personal data** – this is the SCA. **Where an organisation is required by l**aw to process personal data, it **must retain controller responsibility**

Processor means the person who processes personal data on **behalf of the controller**. **For example, any suppliers who adm**inister any systems for the SGB – such as IT/other service providers

4. Data Protection Principles

Anyone processing personal data must comply with the eight principles of good practice. These provide that personal data must be:

1. Processed fairly and lawfully
2. Processed for limited purposes and in an appropriate way
3. Adequate, relevant and not excessive for the purpose
4. Accurate
5. Not kept longer than necessary for the purpose
6. Processed in line with data subjects' rights
7. Secure
8. Not transferred to people or organisations situated in countries without adequate protection

5. Dealing with Subject Access Requests

Data subjects can raise a Subject Access Request in respect of data that an organisation holds concerning them. The GDPR allows a month to comply with this request and there is normally no charge although there is a right to refuse or charge for requests that are manifestly unfounded or excessive. Data subjects can request information to be supplied electronically in a commonly used format rather than in printed form.
If a request is refused the individual must be told the reason for refusal.

6. Dealing with requests to be forgotten

Under the GDPR, subject to certain conditions being met, an individual has the right to have their data erased. If such a request is received from an individual, the SCA as the Data Controller, must assess the request in the context of the personal data that is held and the needs that exist to retain data including legal, commercial, contractual and other factors. In some circumstances, whilst it will be possible to erase some data it may not be possible to erase all data about an individual due to these considerations.

7. Dealing with breaches of personal data

Under the GDPR, the SCA, as a Data Controller, is under obligation to maintain a breach register where all data breaches, no matter how trivial, are recorded and monitored.

For serious data breaches, where the breach is likely to result in a 'risk to the rights and freedoms of individuals', the breach must be reported to the ICO within 72 hours of becoming aware of the breach and the data subject notified without undue delay.

If a volunteer or employee becomes aware of a loss of personal data or a potential breach of security of data they have a legal responsibility to report this to the SCA Data Protection Officer immediately:

- This can be reported to the SCA Data Protection Officer by emailing: sca.dpo@canoescotland.org or they can phone the SCA office if it during office hours (Mon-Fri 08:30-15:30)
- The volunteer/employee should try to get the data back:
    - If they have e.g. sent data in error via email they should contact the recipient and request deletion/safe return of the data
    - If they have e.g. mislaid paper/documents containing personal data they should retrace their steps and do what they can to recover the missing documents
    - If they suspect that someone has accessed data through unauthorised access to an electronic device (computer/tablet/smartphone/online system) they should pass as much information to the SCA Data Protection Officer as possible
    - If an electronic device (computer/tablet/smartphone) has been stolen this should be reported to the Police as well as to the SCA Data Protection Officer

The SCA Data Protection Officer will:
- Log the breach in the SCA Data Breach Register
- Investigate the circumstances that gave rise to the breach
- Quantify the data that has been breached and the likely impact of the breach

- Notify the ICO of the breach within 72 hours (as required by law)
- Where there is “a high risk to the rights and freedoms of individuals” notify the data subject(s) concerned without undue delay
- Investigate how the breach occurred and review/revise procedures and/or arrange additional training in order to reduce the risk of future data breaches

8. Complaints

Any complaints arising concerning the SCA’s handling of data should be raised via the SCA Grievance, Discipline and Appeals Policy – available on the SCA website and by contacting the SCA Office.

9. General

- This policy will be reviewed annually or more frequently should circumstances require in order to maintain its currency and relevance with periodic reports to the SCA Board on the implementation and operation of the policy.

- Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the SCA Chief Executive