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 specified in the Data Protection Act 1998 (the **Act**) and other regulations. The Act imposes restrictions on how the SCA may process personal information, and a breach of the Act could give rise to criminal and civil sanctions as well as bad publicity.

2. Status of the Policy

This policy sets out the SCA's rules on data protection and specifies how the SCA will comply with the eight data protection principles contained in the Act. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal information.

This policy is a condition of employment and therefore any employees, in addition to all others who obtain, handle, process, transport and store personal information including board and committee

members, volunteers, SCA representatives, advisers, consultants, contractors and agents will adhere to the rules of the policy. 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 Chief Executive Officer in the first instance.

3. The meaning of Data Protection Terms

The Act is a complex law and uses technical terminology. It is important that these terms are understood. They are explained below and used throughout this policy.

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom the SCA holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The SCA is the data controller of all personal data used in its activities and undertakings. There can be more than one data controller in respect of the same information. For example, in addition to the SCA, a member club may also be a data controller.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the SCA's data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include board and committee members, volunteers, SCA representatives, advisers, consultants, contractors and agents who handle personal data on the SCA's behalf, for example where SCA has a volunteer inputting a new member's details onto its system.

Data Protection Compliance Officer is the person responsible for the SCA's compliance with the Data Protection Act and the SCA Data Protection Policy. The Compliance Officer is also responsible for handling Subject Access Requests.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in the possession of the SCA). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual's privacy in some way. Mere mention of someone's name in a document does not constitute personal data, but personal details such as someone's contact details, participation details or details of any medical condition would still fall within the scope of the Act.

Processing is any activity that involves use of the data, including simply viewing the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties (even partner organisations).

Sensitive personal data comprises information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. Data Protection Principles

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

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

(i) Fair and Lawful Processing

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told, in a data protection notice, who the data controller is, the purpose for which their data is to be processed by the SCA, and the identities of anyone to whom the data may be disclosed or transferred. In addition, the data protection notice must be given to the data subject at the time the data is obtained and where the personal data is obtained from a third party source e.g. an affiliated club or centre, the data protection notice must be provided as soon as practical after that data is processed. If a member club has already told the individual that their personal data will be passed to the SCA then the SCA need not tell the individual again. The data protection notices must be prominent and legible and included at every point of collection of personal data.

For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interests of the data controller or the party to whom the data is

disclosed. When sensitive personal data are being processed, additional conditions must be met. For example, information concerning a person's health, sex life, political opinions, race, ethnicity or religious beliefs can only be held where the individual has given explicit consent for this or in certain other limited circumstances, for example where the SCA is required by employment law to process such sensitive information. In most cases the data subject's explicit consent to the processing of such data will be required.

(ii) **Processing for Limited Purposes**

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected, which may include, but is not limited to,

(i) the collation of data to produce statistics which will be supplied to, amongst others, government agencies,

(ii) to research, develop and manage new and existing programmes and projects for the strategic development of paddlesport and for promoting paddlesport generally,

(iii) for communicating with individuals about their membership and/or their involvement in programmes, projects, competitions, courses and other activities, and

(iv) providing information to individuals about matters related to paddlesport, activities regarding paddlesport administration and its sponsors) or for any other purposes specifically permitted by the Act.

This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

(iii) **Adequate, Relevant and Non-Excessive Processing**

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

(iv) **Accurate Data**

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be securely destroyed.

(v) **Timely Processing**

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from the SCA's systems when it is no longer required. Information which is held for historical or statistical purposes (such as qualifications, results of competitions etc) can be held indefinitely. Although details of previous members should not be held indefinitely, anonymised information about members (i.e. information which does not identify specific individuals) is not regarded as personal data and can be held indefinitely.)

(vi) **Processing in line with data subject's rights**

Data must be processed in line with data subjects' rights. Data subjects have a right to:-

- Request access to any data held about them by a data controller.

- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

(vii) **Data Security**

The SCA must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires the SCA to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:-

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the SCA central computer system instead of individual PCs.

Security procedures include:-

- **Log On System.** All IT systems have a log on system which allows only authorised personnel access to personal data. Passwords on all computers are changed frequently and must not be disclosed to others.
- **Secure lockable desks and cupboards.** Desks and cupboards are kept locked if they hold confidential information of any kind and can only be accessed by certain individuals. (Personal and financial information and child protection data is always considered confidential and additional security measures are in place for such information.)
- **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
- **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

(viii) **International Transfers**

Personal data should not be transferred to a country outside the European Economic Area unless the country to which the personal data is being transferred provides adequate safeguards. In many cases this will necessitate the data subject consenting to the personal data being transferred.

(ix) **Practical Pointers**

To maintain data security and compliance with the law, data users should:

- when sending emails to more than one data subject (whether by a distribution list or otherwise), consider 'blind copying' each data subject so that each data subject's contact details are not disclosed to the other data subjects.

- ensure that no information is published on the SCA website in respect of a data subject unless the information is already in the public domain or that data subject has been informed and it is reasonable to do so or they have consented to such publication.

- exercise care when disclosing information about someone else. Only do so if the other person has consented or it is reasonable in all the circumstances to comply with the request without the consent of the other person.

7. Dealing with Subject Access Requests

A formal request from a data subject for information the SCA holds about them must be made in writing. Employees, board or committee members, volunteers, the SCA representatives, advisers, consultants, contractors and agents who receive a written request should forward it to the Data Protection Compliance Officer appointed by the SCA immediately. The SCA should respond to the request within 40 calendar days and has the right to charge a fee (presently no more than £10) for this service.

When receiving telephone enquiries, employees, volunteers, board or committee members, SCA representatives, advisers, consultants, contractors and agents should be careful about disclosing any personal information held on SCA systems. In particular they should:-

- check the caller's identity to make sure that information is only given to a person who is entitled to it. A common sense approach should be taken when verifying the identity of the caller. For example, if you personally know the individual and are satisfied that they are calling this ought to be sufficient. If you do not know the caller, you could ask to return their call and ensure that the number given tallies with that on the membership database record for the person. Alternatively if individuals have been issued with a password the information can be released if they correctly disclose their password.

- suggest that the caller put their request in writing where the employee, board or committee member, volunteer, SCA representative, adviser, consultant, contractor or agent is not sure about the caller's identity and where their identity cannot be checked. Alternatively, the individual should be asked to attend in person (and especially if the information is of a sensitive nature).

- Refer to the Data Protection Compliance Officer appointed by the SCA for assistance in difficult situations (for example, where any request might involve disclosing someone else's personal data). Employees, board or committee members, volunteers, SCA representatives, consultants, advisers, contractors and agents should not be bullied into disclosing personal information.

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