DATA PROTECTION POLICY

August 2010

Introduction

The Data Protection Act 1998 (DPA, hereafter referred to as 'the Act') was passed in order to implement the European Directive on data protection and applies to all personal data which is held either electronically or in a manual filing system. The Act commenced on 1st March 2000 with most of its provisions becoming effective on 24th October 2001.

The Scottish Federation for Coarse Angling (SFCA) is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data and to full compliance with the Act. The SFCA will therefore follow procedures that aim to ensure that all elected office bearers and volunteers who have access to any personal data held by or on behalf of the Federation, are fully aware of and abide by their duties and responsibilities under the Act.

Statement of policy

In order to operate efficiently, the SFCA has to collect and use certain information about people such as individual members, sporting participants, organisational volunteers and others, defined as *data subjects* in the Act. Such data must only be processed in accordance with this policy which sets out the purposes for which the SFCA holds and processes personal data. Any breach of the policy may result in the SFCA, as the *Data Controller*, being liable in law for the consequences of the breach. All personal information held must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

The SFCA regards the lawful and correct treatment of personal information as very important to its successful operation and to maintaining confidence between the SFCA, its members and sportscotland. The SFCA will ensure that it treats personal information lawfully and correctly.

To this end the SFCA fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

Principles

All data users must comply with the **eight Data Protection Principles**. The Principles define how data can be legally processed. 'Processing' includes obtaining, recording, holding or storing information and carrying out any operations on the data, including adaptation, alteration, use, disclosure, transfer, erasure, and destruction.

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

6. Personal data shall be processed in accordance with the rights of data subject under the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.
8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The DPA defines both *personal data* and *sensitive personal data*.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Handling of personal/sensitive information

The SFCA will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken;

- The right of access to one's personal information within the statutory 40 days;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, the SFCA will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All elected officers are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All elected officers within the SFCA will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

Status of the Policy

The policy has been approved by a meeting of the SFCA Executive Committee held on ***??*** August 2010 and any breach will be taken seriously and may result in appropriate action. Breach of this policy will constitute behavior which brings the sport and the SFCA into disrepute.

Responsibilities of Committee Members and Data Users

All participants involved in Scottish Coarse Angling, including those involved in the organisation of the sport have a responsibility to ensure compliance with the Act and this Code, and to develop and encourage good information handling practices, within their areas of responsibility. All users of personal data within Scottish Coarse Angling have a responsibility to ensure that they process the data in accordance with the eight Principles and the other conditions set down in the DPA.

In accordance with the SFCA Corporate Governance and Risk Management Policy, the Executive Committee will perform periodic audits to ensure compliance with this Policy and the Act and to ensure that this policy remains up-to-date.

Handling of Personal Data by Constituent Clubs

The use of personal data by clubs is governed by the following

- A club should only use personal data for an Association-related purpose with the knowledge and express consent of an appropriate member of the SFCA Executive Committee.
- The use of Association-notified personal data by clubs should be limited to the minimum consistent with the achievement of Association objectives. Wherever possible data should be de-personalised so that clubs are not able to identify the subject.

The SFCA policy stated above and the regulations are based on the principle that clubs must only use personal data under the guidance of an SFCA Executive Member. A breach of these regulations is an offence against SFCA discipline.

Access to data

The Act gives data subjects a right to access personal data held about them by the SFCA, and allows the SFCA to charge a fee for such access (up to a prescribed maximum). The SFCA will seek to take an approach which facilitates access to their personal data by individuals without them having to make formal subject access requests under the Act, whilst acting within the Data Protection Principles. A record must be kept of all requests for access to personal data.

All formal subject access requests must be responded to within the terms laid down by the Act, and must be notified to the Data Protection Officer as soon as they are received. Any cases of doubt as to whether a request for access to personal data is a subject access request under the Act must be referred to the Data Protection Officer without delay.

The SFCA will normally charge the prescribed maximum fee (currently £10) for subject access requests.

Retention of Data

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. SFCA policy is that all personal information holdings are to be reviewed annually in March. Furthermore, personal data relating to individual members is only to be retained for a period of 6 months after their current membership expires.

Data Transfer

When personal data is transferred internally the recipient must only process the data in a manner consistent with the SFCA's Notification and the original purpose for which the data was collected.

Personal data can only be transferred out of the European Economic Area under certain circumstances. The Act lists the factors to be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. Information published on the Web must be considered to be an export of data outside the EEA.

Data Security

All SFCA users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise.

Data Protection Officer

As the SFCA is a not-for-profit organisation, it is exempt from the requirement to notify the Office of the Information Commissioner that it processes personal data. Should this position change, registration shall be sought prior to the collection or processing of data. Questions related to day to day matters on the operation of the policy and the Act can be dealt with by the SFCA Secretary who is also the SFCA Data Protection Officer.

Further information: www.informationcommissioner.gov.uk