Document Title	Information Security Policy		
Published	May 2015	Version	1
Valid to	March 2018		
Author	Martin Symonds - Head of Member Services		

Scottish Archery Association

Information Security Policy

1 Preliminary matters

Scottish Archery is the trading name of The Scottish Archery Association.

For the purpose of the policy, the following definitions will apply.

'Club' means a constituted club, whose members have affiliated to Archery GB and the SAA. Each club will be administered to by its own Committee

'Director' means a person who has been elected to the Board of the SAA as a director, or a person who has been co-opted on to the Board and assumed the rights and privileges of a director.

'Employee' means any person who is employed by, or on behalf of the SAA on either a temporary or permanent basis.

'Member' has the same meaning as defined in the Articles and Bye-laws of the SAA as current from time to time

'SAA' means the Scottish Archery Association, a Company Limited by Guarantee, no. 389745, registered in Scotland.

2 Introduction

The SAA is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"), which came into force on the 1st March 2000. The SAA will therefore follow procedures that aim to ensure that all Employees, Directors or other Members, who have access to any personal data held by or on behalf of the SAA, are fully aware of and abide by their duties and responsibilities under the Act.

3 Statement of Intent

The SAA intends to fulfil all its obligations under the Data Protection Act 1998, and will ensure that all types of data processing are appropriately notified to the Information Commissioner. The SAA also intends to conduct a periodic review and update of the register entries. It is the aim of the SAA that all appropriate staff are properly trained, fully informed of their obligations under the Data Protection Act 1998 and are aware of their personal liabilities.

Any Employee, Director or Member deliberately acting outside their recognised authority will be subject to the SAA's disciplinary procedures, including dismissal, termination of membership and where appropriate, possibly legal action.

Individuals whose information is held and processed by the SAA can be assured that the SAA will treat their personal data with all due care. It is possible that other legislation may (at times and under certain conditions) override data protection law. Individuals should note that the SAA intends to fulfil all of its legal responsibilities.

This policy document applies only to information covered by the Data Protection Act 1998 and will be

updated/amended in line with applicable law.

4 The principles of data protection

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

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

1. That data;
2. 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:

1. Racial or ethnic origin;
2. Political opinion;
3. Religious or other beliefs;
4. Trade union membership;
5. Physical or mental health or condition;
6. Sexual life;
7. Criminal proceedings or convictions.
8.

5 Handling of personal/sensitive information

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

1. Observe fully conditions regarding the fair collection and use of personal information;
2. Meet its legal obligations to specify the purpose for which information is used;

3. Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
4. Ensure the quality of information used;
5. Apply strict checks to determine the length of time information is held;
6. Take appropriate technical and organisational security measures to safeguard personal information;
7. Ensure that personal information is not transferred abroad without suitable safeguards;
8. Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

To achieve this members will have:

1. The right to be informed that processing is being undertaken;
2. The right of access to one's personal information within the statutory 40 days;
3. The right to prevent processing in certain circumstances;
4. The right to correct, rectify, block or erase information regarded as wrong information.

Requests by members and other individuals regarding their personal information should be made in writing. Any written request received by the SAA shall be forwarded to the Director of Member Services immediately. When receiving telephone enquiries, the SAA will only disclose personal data held if the following conditions are met;

1. A check is carried out confirming the caller's identity to make sure that information is only given to a person who is entitled to it : and
2. The call handler will suggest that the caller put their request in writing if the call handler is not sure about the caller's identity and where their identity cannot be checked.

Appropriate measures will be taken to ensure Employees, Involved Members and Directors will not be bullied or otherwise coerced into disclosing personal information.

6 Data Uses and Processes

The SAA will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of Data Protection law. Any new purposes introduced will, where appropriate, be notified to the individual and, if required by law, their consent will be sought.

The SAA will take appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

All Employees, Directors or Members using personal data within or on behalf of the SAA will be told the limits of their authority to use and disclose such information. The overall accountability for Data Protection is assigned to the SAA's Head of Member Services who will ensure that:

1. All purposes and disclosures are coordinated and consistent.
2. All new purposes are documented and notified to the Information Commissioner
3. All problems can be investigated thoroughly
4.

7 Security of electronic data

The SAA will ensure that all personal data, which is kept in a digital format, is kept secure at all times. To achieve this, where personal data relating to the SAA is kept:

1. All such data will be kept in a password protected files.
2. When using a digital storage medium (e.g. pen drive, CD ROM) which may be accessed by others, all personal data on that medium will be password protected, or the medium will use encryption software to maintain its integrity.

8 Security of paper records

The SAA will ensure that all personal data, which is kept as a paper record, is kept secure at all times. To achieve this, all such paper records will be kept secure in a locked file or cabinet.

9 Sending of personal data to other bodies

The SAA will only disclose personal data to third parties, in accordance with the notification to the Data Commissioner. No personal data will be sent by electronic means, unless it is sent in an encrypted format, to prevent interception by non recipients.

Where emails are being sent to several members at once and their consent has not been given to having their email address disclosed to any other person, other than the originator of that email, then the BCC function will be used to send the email to recipients.

10 Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. The SAA is registered as such. The SAA's registration/notification entry can be viewed on the Information Commissioner's web page at www.ico.gov.uk, registration number Z2476585

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The Head of Members Services will review the Data Protection Registration annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

To this end, any changes made between reviews will be brought to the attention of the Head of Members Services immediately.

11 Application of this policy by clubs

Whilst it is up to each club to decide whether they should register, or apply for exemption from registration, with the Information Commissioners Office, they may wish to adopt this policy as their own.

Each club should adopt as good practice, sections 7, 8 and 9 of this document (security of digital data, paper records and sending of personal information to other bodies).

12 Review and duration

This policy will remain in force for a period of 3 years from date of publication.

Prior to the end of the 3 year period, or earlier if required by any enactment of law, this policy will be reviewed by the Head of Member Services.