

SCOTTISH JUNIOR FOOTBALL ASSOCIATION



DATA PROTECTION POLICY

CONTENTS

Section 1: Introduction

Section 2: Principles

Section 3: Personal Data

Section 4: Sensitive Personal Data

Section 5: Processing Personal Data

Section 6: Rights of Access

Section 7: Exemptions

Section 8: Disclosure of Information

Section 9: Security

1. INTRODUCTION

- 1.1 SJFA is required to process relevant personal data regarding employees and members as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.
- 1.2 Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. In this Policy any reference to employees includes current past or prospective employees.
- 1.3 All members authorise the SJFA to hold data, under cover of the Data Protection Act 1998, in relation to advertising, marketing & public relations, accounts & records, administration of membership records including preparation of teamlines and fundraising.
- 1.4 The SJFA Treasurer/Discipline Secretary will act as Data Protection Compliance Officer.

2. THE PRINCIPLES

- 2.1 Anyone processing personal data must comply with the eight principles of good practice. These provide that personal data must be :
 - 2.1.1 Processed fairly and lawfully;
 - 2.1.2 Processed for limited purposes and in an appropriate way;
 - 2.1.3 Adequate, relevant and not excessive for the purpose;
 - 2.1.4 Accurate;
 - 2.1.5 Not kept longer than necessary for the purpose;
 - 2.1.6 Processed in line with data subjects' rights;
 - 2.1.7 Secure;
 - 2.1.8 Not transferred to people or organisations situated in countries without adequate protection.

3. PERSONAL DATA

- 3.1 Personal data covers both facts and opinions about an individual. The SJFA may process a wide range of personal data of employees and/or members as part of its operation.
- 3.2 This personal data may include (but is not limited to); names and addresses, bank details, disciplinary and attendance records, dates of birth and membership details.

4. SENSITIVE PERSONAL DATA

- 4.1 SJFA may, from time to time, be required to process sensitive personal data regarding an employee and/or a member.
- 4.2 Sensitive personal data includes but is not limited to :
 - 4.2.1 medical information;
 - 4.2.2 data relating to membership;
 - 4.2.3 data relating to disciplinary proceedings;
 - 4.2.4 criminal records and proceedings,
 - 4.2.5 data relating to point 5.2.

- 4.3 Where sensitive personal data is processed by SJFA the explicit consent of the appropriate individual will be required as and when making application for membership.

5. PROCESSING PERSONAL DATA

- 5.1 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.)
- 5.2 SJFA and its Management Committee may hold some or all of the following data about some or all members and others who compete in football under the jurisdiction of SJFA: name, postal and email addresses, phone and fax numbers, year of birth, disclosure information, competition age class, competition results, offices held, skills and qualifications, courses attended and details of officiating at competitions. The data may be held in electronic or paper form.
- 5.3 The data may be obtained directly from an individual person, a member club, a member league or other organisations.
- 5.4 The data is used in organising Junior Football in Scotland and for social purposes, including, but not limited to, mailing of magazines and other literature, publication of competition entries and results, tournaments, coaching, team selection, training and appointment of officials.

6. RIGHTS OF ACCESS

- 6.1 A formal request from a data subject for information SJFA holds about them must be made in writing, signed and addressed to the Data Protection Compliance Officer. Employees, Management Committee or working group/committee members, volunteers, SJFA members, registered officials, advisers, consultants, contractors and agents who receive a written request should forward it to the Data Protection Compliance Officer immediately. SJFA will respond to the request within 40 calendar days and has the right to charge a fee (presently no more than £10) for this service.
- 6.2 When receiving telephone enquiries, employees or SJFA office volunteers, member league officials, member club officials, advisers or consultants should be careful about disclosing any personal information held on SJFA, league or club systems. In particular they should :
- 6.2.1 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;
- 6.2.2 Suggest that the caller put their request in writing where the employees or SJFA office volunteers, member league officials, member club officials, advisers or consultants are not sure about the caller's identity and where their identity cannot be checked. Alternatively, the individual should be asked to attend in person (especially if the information is of a sensitive nature.)

- 6.2.3 Refer to the Data Protection Compliance Officer for assistance in difficult situations (for example, where any request might involve disclosing someone else's personal data). Any employees or SJFA office volunteers, member league officials, member club officials, advisers or consultants should not be bullied into disclosing personal information.

7. EXEMPTIONS

- 7.1 Certain data is exempted from the provisions of the Data Protection Act which includes the following :
 - 7.1.1 The prevention or detection of crime;
 - 7.1.2 The assessment of any tax or duty;
 - 7.1.3 Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the SJFA.
- 7.2 The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the Data Protection Compliance Officer.

8. DISCLOSURE OF INFORMATION

- 8.1 SJFA may receive requests from third parties to disclose personal data it holds about employees, office volunteers, members, etc. SJFA confirms that it will not generally disclose information unless the individual has given their consent or one of the specific exemptions under the Data Protection Act applies.
- 8.2 Where SJFA receives a disclosure request from a third party it will take reasonable steps to verify the identity of the third party before making any disclosure.

9. SECURITY

- 9.1 SJFA will take reasonable steps to ensure that members of staff and office volunteers only have access to personal data relating to employees or members where it is necessary for them to do so.
- 9.2 All employees and office volunteers will be made aware of this policy and their duties under the Data Protection Act. SJFA will ensure that all personal information is held securely and is not accessible to unauthorised persons.
- 9.3 SJFA and its Management Committee shall :
 - 9.3.1 Review the length of time they keep personal data;
 - 9.3.2 Consider the purpose or purposes they hold the information for in deciding whether (and for how long) to retain it;
 - 9.3.3 Securely delete information that is no longer needed for this purpose or these purposes; and
 - 9.3.4 Update, archive or securely delete information if it goes out of date.