

DATA PROTECTION POLICY

Updated: October 2023



Scottish
Volleyball

Data Protection Policy

Introduction

Scottish Volleyball (SV) is committed to ensuring the safety and protection of any personal data, or sensitive personal data, which we process. This includes collection, storage, organising, amendment, deletion and sharing. Personal data refers to any data which can identify a living individual, or which in conjunction with other information likely to come into the possession could identify a living individual. For SV purposes this covers:

- 🌀 Name
- 🌀 Address
- 🌀 Date of Birth
- 🌀 Telephone Number
- 🌀 Email Address
- 🌀 Racial or Ethnic Origin
- 🌀 Religious or Similar Beliefs
- 🌀 Disability

The Data Protection Act 2018 and General Data Protection Regulations

The legislation sets rules for processing data and applies to manual filing records and data held on computers.

SV is a data controller which means we determine the purposes for which personal data is processed. SV may employ data processors, which means any person or organisation other than a direct employee who will process data on our behalf. Under these circumstances SV will ensure the data processor has a valid contract requiring compliance with all existing legislation and SV remains legally liable for the data processing. All data processors will be listed in SV Privacy Statement.

Data protection legislation provides eight data protection principles which require that personal data:

- 🌀 Shall be processed fairly and legally, meaning we are open and transparent about how data will be processed, and a privacy notice must be available.
- 🌀 Shall be processed only for specified and lawful purposes and not be processed in a way which is incompatible with those purposes.
- 🌀 Shall be adequate, relevant, and not excessive for the purposes for which it is collected.
- 🌀 Shall be accurate and kept up to date.
- 🌀 Shall not be kept longer than necessary.
- 🌀 Shall be respectful of individuals' rights.
- 🌀 Shall be kept secure by technical and organisational means against

unauthorised and unlawful processing and against accidental loss, destruction, or damage.

- 🌀 Shall be transferred outside the European Union e.g., through websites, only if privacy is respected.

SV is registered as a data controller with the Information Commissioner's Office (www.ico.org.uk) and must by law keep to these principles. If you believe in any way that SV is not processing personal data in accordance with these principles, please contact SV Chief Executive Officer at info@scottishvolleyball.org or on 0131 556 4633 or write to 48 The Pleasance, Edinburgh, EH8 9TJ.

Purposes for Collecting Personal Data

All personal data provided to SV is processed in accordance with the principles of existing legislation. SV collects personal data for:

- 🌀 Membership services.
- 🌀 Entry to SV events, programmes, squads, or courses.
- 🌀 Monitoring the delivery of SV programmes and resources.
- 🌀 Research, development and evaluation of SV programmes and resources.
- 🌀 Grant funding.
- 🌀 Communication regarding SV work.
- 🌀 Marketing of SV programmes, resources, and registration schemes.
- 🌀 Human resources and employment.

Individuals must be adequately informed, in a manner appropriate to their age and understanding, of how SV will process any personal data collected. If there is an intention to share any personal data with third parties, e.g., sponsors, partners, etc. this must be clearly explained to the individual.

Individuals have the right to access the personal data SV holds on them and correct it if inaccurate. If you would like to receive a copy of this data, please provide a written request evidencing who you are and the information you wish to access to info@scottishvolleyball.org.

Data Processing

Data Processing includes collection, storage and sharing of personal and sensitive personal information. Data must be stored on SV database and/or SV Office 365 suite. Where information is accessed through non-SV computers, tablets etc., the device must have an up to date and currently supported operating system and all devices must be password protected. Staff may choose to access emails and contacts through a mobile phone. Under these circumstances all data must be password protected.

Passing Personal Data onto Third Parties

SV will only disclose information to third parties if explicitly required to do so by relevant legislation. In this case, consent of the individual must be obtained before passing on any information to any third parties other than those involved in the co-ordination of SV programmes.

SV will not collect or compile personally identifying information for dissemination or sale to external parties for marketing purposes or host mailings on behalf of third parties.

Data Retention

SV is conscious of obligations to ensure personal information is relevant, accurate, up to date and not retained for longer than necessary. SV data retention guidelines can be found in the Data Retention Policy.

Data Protection Breaches

Any breach of data protection must be reported immediately to the CEO, or in their absence the Office Manager. Breaches are loss or damage, or potential loss or damage, to data and include such circumstances as loss or damage to a computer or smartphone.

All breaches must be reported to the Information Commissioner's Office within 72 hours, including weekends and nights.