Safe Sport International (SSI) Data Protection Policy

This Data Protection Policy sets out SSI's commitments and obligations when it processes personal data about individuals in the UK. When handling personal data, SSI's Trustees, employees, workers, contractors, volunteers, and supplier staff must do so in a way that allows SSI to meet its commitments and obligations under this policy. Any queries in respect of this Data Protection Policy should be addressed to Safe Sport International's Data Protection contact.

1. INTRODUCTION AND SCOPE

1.1 What is personal data and what is a data subject

Personal data is any information held about an identifiable living individual – also known as a "data subject" - about whom SSI processes personal data. An individual can be identifiable both where SSI holds clear direct identifiers about them, or where SSI can identify the individual by other reliable means, such as by reference to other data held by SSI or which is publicly available.

Data protection rules give some examples of information that are direct identifiers, and must be considered personal data, such as name, an identification number, location data, and online identifiers such as IP address. Other examples include payment information, decisions made about individuals and even opinions they hold, or that are held about them.

Sensitive personal data is any information about health, religion, sex life or orientation, racial or ethnic origin, political opinions, trade union membership, genetic data or biometric data that can uniquely identify a person (such as fingerprints or facial recognition technology). Where this policy discusses sensitive personal data, it also includes information about criminal convictions, or alleged criminal activity, which is governed by very similar rules.

1.2 What is processing?

Processing is any use that SSI – or any third party SSI engages – makes of that data, whether for SSI or for a third party. This is includes creating data, amending it, storing it, sharing it, or even accessing, anonymising, or deleting it.

1.3 What obligations does SSI have?

Where SSI chooses what data will be used and for what purposes, it is a data controller and in charge of ensuring that all data protection requirements are met. For example, SSI is a data controller for the information held about its website users and customers.

As a data controller, SSI has obligations under the General Data Protection Regulation (or "GDPR"), the Data Protection Act 2018 and the Privacy & Electronic Communications Regulations 2003. SSI's obligations under these laws are summarised in this policy.

1.4 What are the obligations of SSI Trustees, employees, workers, contractors, volunteers, and supplier staff?

All of SSI's Trustees, employees, workers, contractors, volunteers (insofar as applicable to their role) and supplier staff must assist SSI in complying with this Data Protection Policy and have a duty to respect the commitments, procedures and practices set forth in this Policy and any associated policies.

2. CLASSES OF DATA SUBJECT AND PERSONAL DATA TRANSFERRED

SSI processes and transfers the following categories of personal data, including sensitive personal data, relating to the following classes of data subjects:

- Employees: this includes information such as health records, benefit information, staff development records, attendance records (including any absences due to illness), salary and expenses information, equal opportunities management, disciplinary procedures, employee share holdings, names, addresses, date of birth, employee performance, trade union membership, and next of kin.

- Customer Information: this includes information such as contact information of customers, including name, address and telephone numbers, as well as payment details.

- Anonymized/Aggregated data: SSI may also process anonymized and/or aggregated data for the purposes set out in this policy.

3. CORE DATA PROTECTION PRINCIPLES

SSI observes the following principles when collecting, processing, and transferring personal data:

3.1 Fairness and Lawfulness

Where SSI acts as a data controller, it will only process personal data fairly and lawfully and in particular it must have a legal basis for processing personal data. Examples of a relevant legal basis for processing include:

a) the data subject has given consent;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which SSI is subject; or

d) processing is necessary for the purposes of the legitimate interests pursued by SSI or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, where the data subject is a minor under 13 years (SSI will carry out a balancing test to ensure its legitimate interests justify the intrusion and outweigh any contrary interests of the data subject).

Specific conditions apply to the collection of sensitive personal data. Where SSI acts as a data controller, it is not allowed to process sensitive personal data unless at least one condition of the following for lawful processing of sensitive personal data applies:

a) the data subject has given explicit consent;

b) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent;

c) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of SSI or of the data subject in the field of employment and social security and social protection law;

d) processing relates to personal data which are manifestly made public by the data subject; or

e) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

The treatment of personal data about criminal convictions and offences will vary between jurisdictions. Such data may be processed by SSI only where the processing is authorised by a specific law that provides appropriate safeguards.

3.2 Transparency

When SSI collects personal data as a data controller from data subjects SSI shall inform them of:

a) the identity and the contact details of SSI;

b) the purposes and the legal basis for the processing;

c) the legitimate interest of SSI;

d) the recipients or categories of recipients of the personal data, if any;

e) any international data transfers, including the location of any recipients and the methods used to ensure the adequate protection of those transfers (and how to obtain details of those methods);

f) data retention periods (if applicable);

g) their rights under data protection rules;

h) the process available to data subjects to withdraw any consent;

i) whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data; and

j) the existence of automated decision-making, if any, including profiling, and the logic involved.

When SSI acts as a data controller for personal data collected from any other source, or creates the data itself, it will additionally inform the data subject about the source of the personal data. This information should be as precise as possible.

SSI should provide this information at the time it collects the data from the data subject, or if it collects the data from another source, it should provide this information within a reasonable period. If SSI intends to communicate with the data subject, or disclose the data to a third party, then information is to be provided no later than that communication or disclosure.

Privacy notices will be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language (in particular where the data subject is a child). The information will be provided in writing, or by other means, including, where appropriate, by electronic means.

Where the provision of information proves impossible or would involve a disproportionate effort and data is not being obtained directly from the data subject, SSI may instead include details of the processing in a public facing policy.

In exceptional circumstances (for example to prevent harm to a third party), the provision of specific information may be postponed or omitted.

SSI's main privacy notice can be found on its website: www.safesportinternational.com.

Where carrying out any new processing, or making a change to any existing processing, consideration should be given as to whether a change to the privacy notice (or a new privacy notice) is required.

3.3 Purpose Limitation and Data Minimization

SSI will process personal data only for the purposes for which it was originally collected. SSI cannot further process personal data in a manner that is incompatible with the original purpose unless an exception is provided under law or a new consent has been obtained from the data subject.

SSI shall process only adequate, relevant and limited personal data of data subjects, ensuring that only data that is necessary in relation to the purposes stated above is processed and retained by SSI. SSI has put in place appropriate measures to ensure privacy by design and default. These are discussed in more detail in the "Accountability" section below.

3.4. Accuracy

SSI will ensure that information is accurately recorded and kept up to date. Data subjects also have a right to correct information that SSI holds about them. Where this is objective information, SSI takes steps to ensure that its methods of collecting data (both directly and indirectly) ensure that data is accurate (for example, by providing clear collection forms, taking steps to automate data collection to reduce transcription errors and putting in place systems to reduce duplication). Individuals must be given opportunities to view and update their information where necessary. Where information is subjective, and SSI does not agree with the change, SSI will record the data subject's views and disagreement.

Particular care is to be taken to ensure that data is recorded accurately, and ensure that prompt responses are provided where a request is received to update or correct information.

3.5 Storage Limitation

SSI will keep personal data in an identifiable form for no longer than is necessary for the purposes that SSI has collected and processed it. Specific details in respect of the retention periods that SSI has adopted for its different purposes and processing activities are set out in SSI's privacy policies and records of processing. For example, SSI's HR data is held for at least 6 years after employment, and as long as is required to meet specific legal requirements, such as health and safety rules. Any Safeguarding complaints will be retained for 75 years. These periods are reviewed as necessary to ensure that appropriate periods have been identified.

Where a retention period is reached, SSI is committed to taking appropriate action to ensure that the relevant data is no longer processed by SSI in an identifiable form. This may involve deleting the data, returning it to the data subject or elected third party, or anonymising the data, depending on what is most appropriate.

3.6 Integrity and Confidentiality

SSI will only collect, process and disclose personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised of unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Personal data breach management

SSI is also required to log and, where necessary, report any personal data breaches.

A personal data breach means a breach of security leading to the accidental, unauthorised or unlawful:

(a) disclosure of, or access to, personal data (a **confidentiality breach**);

(b) alteration of personal data (an **integrity breach**); and/or

(c) destruction of, or loss of access to, personal data (an **availability breach**). An availability breach includes an unplanned system outage that result in a temporary loss of access to personal data.

Personal data breaches can be the result of both accidental and deliberate causes. Where we remain unsure that a breach has occurred, we refer to the potential breach as a data incident. Examples of potential personal data breaches are:

Confidentiality breach
• Loss of an asset (such as a laptop or USB) or documents containing personal data • Unauthorised or accidental disclosures to third parties or the media • Security incidents leading to unauthorised or unlawful access to personal data
Integrity breach
• Data amended, either accidentally or deliberately, affecting the accuracy of information (either permanently, or for a period of time)
Availability breach
• Personal data made unavailable (either permanently, or for a period of time) by system failure, denial of service attack or ransomware, particularly where this affects ongoing services to, or affecting, individuals • Personal data deleted, either accidentally or deliberately, either permanently or unrecoverable for a period of time.

If any SSI employee, worker, contractor, or supplier staff becomes aware of any potential personal data breach, they must immediately inform the SSI Data Protection contact and take any steps available to stop any ongoing risk to individuals.

All organisations, including SSI, must report certain types of personal data breach to the relevant supervisory authority – in almost all cases, this will be the ICO. **This must be done within 72 hours of becoming aware of the breach.**

SSI must provide the supervisory authority with particular information about a personal data breach, such as the nature of the data involved, the nature and number of individuals affected, the likely consequences of the personal data breach and the steps we've taken to mitigate risks.

If the breach is likely to result in a high risk to an individual's rights and freedoms, those individuals must be informed without undue delay.

SSI's Trustees, employees, workers, contractors, volunteers, and supplier staff must report any potential personal data breach to the SSI Data Protection contact and to assist, as requested, with providing further information and assistance in managing any breach. The following information should be provided as part of any report:

• What has happened?
• When and how you became aware of the data incident?
• Where the data incident occurred and which, if any, systems it affects?
• Are you aware of third party involvement (whether this is processors, other tennis or broadcast stakeholders or unknown third party actors)?
• What is the nature of the data involved, and does this involve any sensitive personal data?
• Which individuals are affected (particularly their number and their relationship with SSI)?

• Is there any ongoing risk to individuals or their data?
• What security measures were in place, if any?
• What consequences, if any, are you aware of any this time?

Engaging or sharing data with third parties

Where SSI deals with third parties, it may need to enter into written agreements with those third parties to ensure that any personal data which is shared as part of that relationship is appropriately protected – whether that third party is a data controller or a data processor.

3.7 Accountability and Data Governance

SSI wishes demonstrate compliance with the principles set out above. The processes and procedures adopted by SSI to ensure and document compliance include the following:

- Privacy by design and default: When acting as a Data Controller, SSI will consider the privacy implications of any new processing and any changes it makes to how it processes personal data.

- Data Protection Impact Assessments ("DPIA"): When acting as Data Controller, SSI will run DPIAs on any "high risk" processing activity before it is commenced. DPIAs will include a description of the processing activities and their purpose and an assessment of the need for and proportionality of the processing, the risks arising and measures adopted to mitigate those risks, in particular safeguards and security measures to protect personal data and comply with the law.

- Records of processing: SSI keeps a record of its processing activities of personal data (including the type of personal data processed, the relevant data subject, and the purposes for which it is used) which it carries out both as a data controller and as a data processor. These records of processing are reviewed whenever existing processing is changed or new processing takes place, and any relevant updates are made. Major updates are made on an ad-hoc basis where required.

4. DATA SUBJECT RIGHTS

Data subjects can exercise their rights under the law at any time by contacting SSI by using the contact details set out in the relevant privacy notice or otherwise getting in touch with SSI. Data subjects are entitled to use any means to make requests to SSI – these can be oral as well as written requests. The rights available to data subjects are as follows:

- Rights of access and portability: SSI must, on request from a data subject: (i) confirm if SSI processes relevant personal data; (ii) provide a copy of the personal data (in commonly used electronic form in many cases); and (iii) provide supporting explanatory materials. For personal data provided by the data subject which is processed automatically, and which SSI processes with the individual's consent or to fulfil a contract with that individual, SSI must "port" the relevant personal data to a new service provider if so requested, or make the relevant personal data available to the individual, in machine readable and structured format. Relevant exemptions may exist to such disclosures, particularly where disclosures would adversely affect the rights and freedoms of others.

- Right of rectification: SSI will consider and, where required, comply with requests from data subjects to rectify inaccurate personal data. SSI shall only process accurate personal data and they shall verify that personal data is kept up-to-date. If a data subject submits a valid claim that the personal data SSI maintains about them is incorrect, SSI must work to rectify the inaccuracy. If SSI disagrees with the individual, it will retain a record of the individual's disagreement over accuracy.

- Right of objection: SSI will consider and, where required, comply with requests from data subjects to object to: (i) direct marketing; (ii) scientific, historical or statistical research; and/or (ii) processing justified based on legitimate interests;

- Right of erasure (the "right to be forgotten"): SSI will consider and, where required, comply with requests from data subjects for their personal data to be "erased". SSI must comply with such requests when there is a problem with the underlying legality of the processing or where the processing was based on consent and this consent has been withdrawn, or where the data subject has validly exercised a right to object and wishes the data to be erased.

- Right of restriction: SSI will consider and, where required, comply with requests from data subjects to "restrict" the processing of personal data whilst complaints (for example, about accuracy) are resolved, or if the processing is unlawful but the data subject objects to erasure.

- Automated decision-taking: SSI will not take decisions based solely on the automated processing (i.e. with no human involvement) of a data subject's personal data which produce legal effects, or have similarly significant effects, unless permitted by law.

5. SHARING DATA WITH THIRD PARTIES

Any third party appointed to collect, store or use personal data as SSI's data processor must provide satisfactory assurances and contractual commitments as required by the applicable law. Third parties acting as data processors will be subject to a data protection and information security risk assessment before they start providing any service. Third parties who act as SSI's data processor must enter into a written agreement with SSI which ensures that it will provide adequate privacy, data protection and information security measures. Such agreements shall include, at a minimum, certain contractual safeguards, including clear details on what data the third party is processing on the SSI's behalf and what processing service they are providing.

Where SSI transfers personal data from data subjects to third parties acting as data processors that are (i) located in countries that do not provide adequate levels of protection (ii) not covered by approved binding corporate rules; or (iii) who do not have other arrangements that would satisfy UK adequacy requirements, SSI will ensure that appropriate contractual controls, such as model contractual clauses are implemented unless an appropriate exemption exists.

When SSI shares personal data with third parties that are also data controllers, SSI will ensure that there is a legal basis under the applicable law for such data sharing and will implement appropriate measures to address any relevant data transfers outside the UK to such third parties unless an appropriate exemption exists.

In accordance with applicable law, treaties or applicable international conventions, SSI may share personal data with law enforcement and regulatory agencies when necessary in a democratic society to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, and, in particular to comply with sanctions as laid down in international and/or national instruments, tax-reporting requirements or anti-money-laundering reporting requirements.

6. AWARENESS

SSI will take steps to ensure that its employees, workers, contractors, volunteers, and (as appropriate) supplier staff are aware of the requirements of this Data Protection Policy and SSI's expectations in respect of data protection.

7. UPDATES

SSI will circulate any updates to this policy as necessary from time to time.