FREE STATE

ACADEMY OF SPORT

Protection of Personal Information Policy

1. POLICY SCOPE

This policy provides guidance on how the FSAS will manage its legal obligations and requirements concerning confidentiality and personal information security. The requirements with this Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013, as amended.

2. POLICY STATEMENT

The FS Academy of Sport collects and use personal information of their clients and stakeholders with whom it works in order to operate and carry out its business effectively.

The FSAS regards the lawful and appropriate processing of all personal information as crucial to ensure successful service delivery and essential to maintain confidence between the FSAS and its clients and stakeholders.

3. PROCESSING OF PERSONAL INFORMATION

The FSAS uses personal information of its clients under its care in the following way:

- Providing programmes and services to clients
- Administration of agreements
- Conducting market or customer satisfaction research
- Marketing of services and programmes
- In connection with legal proceedings
- Staff administration
- Keeping of records & accounts
- Compliance with legal and regulatory requirements
- Profiling of clients for the purpose of marketing

The FS Academy of Sport may possess records relating to its clients, stakeholders, service providers and staff as follows:

Names, contact details, physical and postal address, date of birth, ID number, nationality and gender, Tax related information, financial information, and banking details.

The FSAS may share the personal information with its stakeholders who may use this information to send clients information on products and services.

The FSAS may supply the personal information to any party or entity to whom the FSAS have assigned or transferred its rights or obligations under any agreement and/or service provider who render the following services:

- Capturing and organising data
- Storing of data
- Sending of e-mails and other correspondence to clients

The FSAS may retain personal information records unless clients and/or stakeholders objects thereto. If clients and/or stakeholders object to indefinite retention of its personal information, the FSAS shall retain the personal information records to the extent permitted or required by law.

The FSAS uses up to date technology to ensure the confidentiality, integrity, and availability of personal information under its care, which includes:

- Firewalls
- Virus protection software and update protocols
- Physical access control
- Secure setup of hardware and software
- Outsourced service providers are contracted to implement security controls

4. PROCESSING OF INFORMATION CONDITIONS

The FSAS shall ensure that all processing conditions as set out in the Protection of Personal Information Act, No.4 of 2013 (as amended), are complied with when determining the purpose and means of personal information and during the processing thereof. The FSAS shall remain liable for compliance with these conditions, even it has outsourced its processing activities.

The processing of personal information is only lawful if, given the purpose of processing, the information is adequate, relevant, and not excessive.

The FSAS must collect personal information directly from clients and stakeholders, unless:

- The personal information is contained in a public record
- The personal information has been made public by its clients and stakeholders
- The personal information was collected from another source with the client's consent and without any prejudice to the client
- Collection of personal information from another source is necessary to maintain and/or comply with or exercise any law or legal right

The FSAS shall take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated. The FSAS will periodically review personal information records to ensure that personal information is still valid and correct.

The FSAS shall as far as reasonably practical, follow the following guidance when collecting personal information:

- Personal information shall be dated when received
- A record shall be kept from where the personal information was obtained
- Changes to personal information records shall be dated
- Irrelevant personal information shall be deleted or destroyed
- Personal information records shall be stored securely, either on a secure electronic database or in a secure physical filing system

The FSAS shall take reasonable steps to ensure that clients and stakeholders are made aware of the following:

- what personal information is collected and the source of the information
- the purpose of collecting and processing of personal information
- the supply of personal information is voluntary or mandatory, and the consequences of failure to provide such information
- the collection of personal information is in terms of any law requirements
- Whether the personal information obtained shall be shared with any third party

Clients and/or stakeholders have the right to request access to, amend or delete their personal information. All such requests must be submitted in writing to the FSAS, including adequate proof of identity of the client/stakeholder, and allowing the Academy reasonable time to respond. The FSAS shall not disclose any personal information to any party unless the identity of the requester has been verified.

The FSAS shall ensure the integrity and confidentiality of all personal information in its possession, by taking reasonable steps by identifying reasonable foreseeable risks to information security and establish and maintain appropriate safeguards against such risks.

Written personal information records shall be kept in files in a designated officials' office which will be kept locked and not left unattended in areas where non-staff members may access them. Officials shall be required to clear their desks of all personal information when leaving their desks for any length of time and at the end of the day. Personal information which is no longer required should be disposed of by shredding.

All electronically held personal information must be saved in a secure database and all computer equipment should be access protected with a password. Officials shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day. Electronic personal information which is no longer required must be permanently deleted from the relevant database and computer.