Information and Technology Manual

Protection of Personal Information Policy

Document Custodian	**Chief Executive**
Document Compiler	**Chief Operations Executive**
Document Quality Reviewer	**QMS and Risk Officer**
Implementation Responsibility	**Chief Operations Executive**
Document Control Number:	**PO107**
Version Control Number:	**Version 01**
Date of Approval:	**24 June 2021**
Effective Date:	
Review Date:	**24 June 2021**
Related Documents:	**IT Security Policy, Data Management Policy, Information Management and Disposal Policy Employee Relations Policy, Code of Business Ethics. Website Privacy Notice, Employee Privacy notice, Delegate Privacy Notice.**
Number of Pages (Inclusive)	**Eleven (11)**

1. PURPOSE

1.1. The purpose of this policy is to explain the manner in which the South African Institute of Professional Accountants ('SAIPA™') deals with personal information of Data subjects, and in addition, the purpose for which this information is used.

1.2. This policy also serves to protect SAIPA from compliance risks associated with the protection of personal information which includes:

a) Breaches of confidentiality

b) Failing to offer choice to Data subjects to choose how and for what purpose theirinformation is used.

c) Reputational damage.

1.3. The policy also demonstrates SAIPA's commitment to protecting the privacy rights of Data subjects.

2. SCOPE

This document applies to SAIPA's Board and Committee members, all employees, contractors, suppliers, clients, persons acting on behalf of SAIPA and all potential and existing Data subjects.

3. INTRODUCTION

3.1. The Protection of Personal Information Act, 4 of 2013 ('POPIA') requires SAIPA to inform Data subjects as to how their personal information is used, disclosed and destroyed.

3.2. SAIPA is committed to compliance with POPIA and other applicable legislation, protecting the privacy of Data subjects and ensuring that their personal information is used appropriately, transparently and securely.

3.3. This policy is made available on SAIPA's website www.saipa.co.za and should be read in conjunction with SAIPA's IT Security Policy, Data Management Policy, Information Management and Disposal Policy Employee Relations Policy, Code of Business Ethics. Website Privacy Notice, Employee Privacy notice, Delegate Privacy Notice.

4. DEFINITIONS

4.1. Personal Information

4.1.1. Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an existing, identifiable juristic person and may include but is not limited to:

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

b) information relating to the education or the medical, financial, criminal or employment history of the person;

c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

d) the biometric information of the person;

e) the personal opinions, views or preferences of the person;

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

g) information regarded as confidential business information;

h) the views or opinions of another individual about the person; and

i) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

4.2. Data subject

This refers to the natural or juristic person to whom personal information relates, such as Members, Accredited Training Centres (ATCs), employees, clients, delegates, sub-contractors or a company that supplies SAIPA with goods or services.

4.3. Processing

The act of processing information includes any activity or set of operations concerning personal information and includes:

a) the collection, receipt, capturing, collation, storage, updating, retrieval, alteration or use;
b) dissemination by means of transmission, distribution or making available in any otherform; or
c) merging, linking, erasure or destruction of information.

5. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of SAIPA will be subject to the following guiding principles:

5.1. Accountability

Compliance failure could damage the reputation of SAIPA and its shareholders. SAIPA could also be exposed to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

SAIPA will take appropriate steps including disciplinary action against individuals who through intentional or negligent actions and/or omissions fail to comply with this policy.

5.2. Processing limitation

5.2.1. SAIPA collects personal information directly from Data subjects only as

pertains to business requirements. The type of information will depend on the need for which it is collected and will be processed for that purpose only. SAIPA informs Data subjects as to what information is mandatory or deemed optional, as far as possible.

5.2.2. Personal information will only be used for the purpose for which it was collected, intended and as agreed. This may include:

a) Processing applications for Membership in any of the SAIPA categories

b) Processing applications to attend CPDs, webinars, events, conferences, RFPs, etc;

c) Issuing certificates to delegates upon successful completion of PE Examinations;

d) Processing claims received from service providers;

e) Issuing tax certificates to service providers;

f) Recruitment activities;

g) Record-keeping and payment of employees and service providers;

h) Administration of employment benefits;

i) Recording and payment of service providers;

j) Confirming, verifying and updating member information;

k) For registration purposes with statutory bodies (CIPC, SARS) and institutions (banks);

l) Contractual obligations;

m) In connection with legal proceedings;

n) In connection with and to comply with legal and regulatory requirements or when allowed by law;

o) For audit and reporting purposes; and

p) Marketing activities.

5.2.3. According to Section 10 of POPIA, personal information may only be processed if the purpose for which it is processed, is adequate, relevant and not excessive. Certain conditions must be met for SAIPA to process personal information as in Section 11 of POPIA. These are listed below:

a) Data subjects' consent to the processing – consent is obtained at the point of applying for membership, or in a manner that may be necessary for the performance of any of the activities listed in section 5.2.2 above.

b) Processing is necessary – personal information is required to facilitate

the provision of services to the Data subject or for the conclusion of a contract to which the Data subject is a party, inclusive of Personal Indemnity (PI) Insurance.

c) SAIPA is under obligation by law.

d) The legitimate interest of the Data subject is protected – it is in the Data Subject's best interest to provide the personal information to SAIPA.

e) Processing is in the best interest of SAIPA – in order to provide our services to the Data subject.

5.3. Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Where the secondary purpose is not compatible with the original purpose, SAIPA will first obtain additional consent from the Data subject.

5.4. Information quality

SAIPA will take reasonable steps to ensure that all personal information is complete, accurate and not misleading. Where personal information is collected from third parties, SAIPA will take all reasonable and necessary steps to ensure that the information is accurate and correct. This may include SAIPA verifying the accuracy of the information directly with the Data subject or through confirmation from third party sources authorised to possess such information (including but not limited to entities such as SAQA; and CIPC).

5.5. Openness

5.5.1. When personal information is collected, reasonable steps shall be taken to ensure that the data subject is aware of –

a) the information being collected and where the information is not collected from the data subject, the source from which it is collected;

b) the name and address of the responsible party;

c) the purpose for which the information is being collected;

d) whether or not the supply of the information by that data subject is voluntary or mandatory;

e) the consequences of failure to provide the information;

f) any particular law authorising or requiring the collection of the information;

g) the fact that, where applicable, SAIPA intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation.

5.5.2. The aforementioned notification should include notification of the rights of the data subject concerned which include the right:

a) to be notified that—
   i. personal information about the data subject is being collected as provided for in terms of section 18 of the POPIA; or
   ii. the data subject's personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22 of the POPIA;

b) to establish whether a responsible party holds personal information of that data subject and to request access to their personal information as provided for in terms of section 23;

c) to request, where necessary, the correction, destruction or deletion of their personal information as provided for in terms of section 24 of the POPIA;

d) to object, on reasonable grounds relating to their particular situation to the processing of their personal information as provided for in terms of section 11(3)(a) of the POPIA;

e) to object to the processing of their personal information—
   i. at any time for purposes of direct marketing in terms of section 11(3)(b) of the POPIA; or
   ii. in terms of section 69(3)(c) of the POPIA;

f) not to have their personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1) of the POPIA;

g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of their personal information intended to provide a profile of such person as provided for in terms of section 71 of the POPIA;

h) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74 of the POPIA; and

i) to institute civil proceedings regarding the alleged interference with the protection of their personal information as provided for in section 99 of the POPIA.

5.5.3. The aforesaid notices shall remain an integrate part of all SAIPA terms and conditions in terms of which SAIPA engages members and the public at large. The acceptance of these terms and conditions will form the basis of consent for the collection and processing of personal information. Additionally, should SAIPA receive any personal information without prior consent thereto, a notification which encompasses the detail contained above must be dispatched to the data subject in question as soon as

possible.

5.5.4. The requirement as detailed above will however not need to be complied with where:

a) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;

b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of the Act;

c) non-compliance is necessary—

i. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

ii. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

iii. for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

iv. in the interests of national security;

d) compliance would prejudice a lawful purpose of the collection;

e) compliance is not reasonably practicable in the circumstances of the particular case; or

f) the information will—

i. not be used in a form in which the data subject may be identified; or

ii. be used for historical, statistical or research purposes.

5.6. Security safeguards

5.6.1. in order to comply with the provisions of the Act, the appropriate technical and organisational measures shall be taken to prevent any loss of, damage to or unauthorised destruction or access to personal information in SAIPA's possession. This will necessitate that a risk assessment be conducted in terms of which all internal and external risks to the comprise of personal information are identified, the appropriate risk mitigation steps are taken to address these risks and that risk and risk mitigations steps are continually assessed to ensure provision is made for both existing and emerging risks.

5.6.2. In the event that third parties are granted access to personal information in SAIPA's possession, SAIPA shall ensure that same is done in accordance with a written agreement in terms of which the dedicates of both this policy and the Act are contained and further in terms of which such third explicitly agrees to comply therewith.

5.6.3. In the event that SAIPA becomes aware or reasonably suspects that personal

information in its possession has been compromised, SAIPA shall as soon as reasonably practicable, notify both the Information Regulator and the data subject of such breach.

5.6.4. Notification to the data subject concerned shall be done in writing through both email correspondence as well as notification posted on the data subject 's MySAIPA profile.

5.6.5. such notification to the member shall contain the following:

a) A description of the possible consequences of the breach;

b) The measures SAIPA has taken/intends on taking to address the breach;

c) A recommendation on the steps the data subject should take to mitigate any adverse effects from the breach; and

d) The identity of the person who committed the breach if the identity of such person is known to SAIPA.

5.7. Data Subject Participation

5.7.1. Data subjects are entitled to request confirmation from SAIPA as to whether SAIPA holds personal information of that data subject and further the right to request a record of such information. Such record shall be provided to the data subject within a reasonable time after the request is received and shall be a format readable by the data subject.

5.7.2. A data subject further has the right to request the amendment or destruction of the inaccurate or out of date personal information held by SAIPA and SAIPA shall amend or delete such information, in accordance with the instructions of the data subject concerned, as soon as reasonably practical after receipt of such instruction.

6. SPECIFIC DUTIES AND RESPONSIBILITIES

6.1. SAIPA Board

SAIPA's Board is ultimately accountable for ensuring that SAIPA meets its obligations under POPIA. The Board may however delegate some of its responsibilities to management or other capable individuals.

6.2. SAIPA's Information Officer is responsible for the following:

a) Taking steps to ensure SAIPA's reasonable compliance to POPIA;

b) Keeping the Board informed of SAIPA's information protection responsibilities, for instance in the case of a security breach;

c) Reviewing SAIPA's information protection procedures and policies;

d) Ensuring that SAIPA makes it convenient for Data subjects to communicate with SAIPA regarding their personal information;

e) Approve any contracts entered into which may have an impact on personal information held by SAIPA;

f) Oversee the amendment of employment contracts and other service level

agreements;

g) Encourage compliance with the lawful processing of personal information;

h) Ensure that employees and persons acting on behalf of SAIPA are aware of the risks associated with the processing of personal information;

i) Ensure that employees are trained in the processing of personal information;

j) Address employees' POPIA related questions;

k) Address POPIA related requests and complaints made by SAIPA's Data subjects;

l) Act as contact point for the Information Regulator on issues pertaining to the processing of personal information;

m) Addressing any personal information protection queries from media.

6.3. SAIPA's Manager in charge of Information Technology is responsible for:

a) Ensuring that SAIPA's IT infrastructure and any other devices used for processing personal information meet acceptable security standards;

b) Ensuring that servers containing personal information are sited in a secure location;

c) Ensuring that all electronically stored information is backed-up and tested on a regular basis;

d) Ensuring that all back-ups are protected from unauthorised access, accidental deletion and malicious hacking attempts;

e) Ensuring that information being transferred electronically is encrypted;

f) Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software;

g) Performing regular IT audits to ensure that the security of SAIPA's hardware and software systems are functioning properly;

h) Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by unauthorised persons; and

i) Performing a proper due diligence review prior to contracting with third party providers to process personal information on SAIPA's behalf.

6.4. SAIPA's Chief Operations Executive (COE) is responsible for:

a) Approving and maintaining the protection of personal information statements and disclaimers that are displayed on SAIPA's website, including those attached to communications such as emails and electronic newsletters;

b) Work with persons acting on behalf of SAIPA to ensure that any outsourced marketing initiatives comply with POPIA.

c) Ensuring that the human resource and payroll system is POPIA compliant;

d) Providing assurance of good privacy practices applied in the Institute; and

e) Authorising access rights to the human resource and payroll systems.

6.5. Employees and other persons acting on behalf of SAIPA are responsible for:

a) Keeping all personal information that they come into contact with secure by taking precautions and complying with this policy;

b) Ensuring that personal information is kept in as few places as is necessary;

c) Ensuring that personal information is encrypted prior to sharing the information electronically;

d) Ensuring that all devices such as computers, flash drives, etc. are password protected and never left unattended (refer to SAIPA's IT Security policy);

e) Ensure that computer screens and other devices are switched off when not in use;

f) Ensure that removable storage devices such as external drives that contain personal information are locked away securely when not being used;

g) Ensure that where personal information is stored on paper, that such hard copies are kept in a secure place where unauthorised persons are not able to access it;

h) Ensure that where personal information has been printed out, that the printouts are not left unattended where unauthorised individuals could see them;

i) Take reasonable steps to ensure that personal information is stored only for as long as it is needed or required; and

j) Undergo POPIA awareness training from time to time.

Employees and other persons acting on behalf of SAIPA will under no circumstances:

a) Process personal information where it is not a requirement to perform their work-related duties;

b) Save copies of personal information directly to their own private computers or mobile devices; and

c) Share personal information informally.

When an employee, or a person acting on behalf of SAIPA, becomes aware or suspicious of any security breach of personal information, he or she must immediately report this to the Information Officer.

7. DISCIPLINARY ACTION

7.1. SAIPA may recommend appropriate legal or disciplinary action to be taken against any employee found to be implicated in any non-compliant activity outlined within this policy.

7.2. Any gross negligence or intentional mismanagement of personal information will be considered a serious form of misconduct under SAIPA's Employee Relations Policy and Code of Ethical Conduct and may lead to dismissal.

7.3. Examples of actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to law enforcement agencies for criminal investigation
- Recovery of funds in order to limit any damages caused.

7.4. The detail of SAIPA's Information Officer is as follows:

Name	Mr Shahied Daniels
Telephone number	011 207 7840
Postal Address	P O Box 2407 Halfway House 1685
Physical Address	SAIPA House, Howick Close, Waterfall Park Vorna Valley, Midrand 1685
E-Mail Address	ceo@saipa.co.za

8. POLICY APPROVAL

This Protection of Personal Information Policy is hereby adopted and approved for implementation and takes effect upon signature by the SAIPA Chief Executive

Signed on this ……. day of …….... 2021 at ……**MIDRAND**.....

…….
Dr Gavin G Isaacs
Chief Operations Executive

…….
Mr S Daniels
Chief Executive