POPI ACT PROCEDURE & POLICY

ASDSA
ASSOCIATION FOR SKILLS DEVELOPMENT IN SOUTH AFRICA

*The Association for Skills Development in South Africa Herein After referred to as **ASDSA***

Version Number:	2021/01

Approval Process

RESPONSIBLE PERSON	NAME	SIGNATURE	DATE
NATIONAL CHAIRPERSON	Sharon Van den Heever		30.05.2022
HEAD OF LEGAL RISK & COMPLIANCE	Sharon Van den Heever		30.05.2022
TREASURER	Andy Reinecke		30.05.2022
BOARD MEMBER	Maryna Ritter		30.05.2022

1. REVIEW REGISTER

It is advisable to review the policy on an annual basis. Any amendments must be indicated on the document review roster and relevant staff members must be informed of any updates.

Revision Record Sheet

Rev No:	Description of revision	Rev date
1	First Draft June 2021	**June 21 – May 22**
2		
3		
4		
5		
6		

2. STAFF CONFIRMATION SHEET

I confirm that I have read and understand the contents of this document and that I am aware of my duties in respect thereof		
Sharon Van Den Heever	**30.05.2022**	
Name	**Date**	**Signature**

3. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner. Through the provision of quality goods and services, **ASDSA** is necessarily involved in the

collection, use and disclosure of certain aspects of the personal information of Members, Designees, Agents, volunteers and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions. Given the importance of privacy, **ASDSA** is committed to effectively managing personal information in accordance with POPIA's provisions.

4. DEFINITIONS[AR1]

4.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a member), including, but not limited to information concerning:

a) race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person
b) information relating to the education or the medical, financial, criminal or employment history of the person
c) any identifying number, symbol, email 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) the views or opinions of another individual about the person
h) 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 an individual member; designee or a company that supplies the professional body with services or other goods.

4.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the professional body is the responsible party.

4.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the professional body to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

4.5 Information Officer

The Information Officer is responsible for ensuring the professional body's compliance with POPIA. Where no Information Officer is appointed, the head of the professional body will be responsible for performing the Information Officer's duties. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

4.6 Processing

The act of processing information includes any activity or any set of operations, whether or not BY automatic means, concerning personal information and includes:

a) the collection, receipt, recording, professional body, collation, storage, updating or modification, retrieval, alteration, consultation or use
b) dissemination by means of transmission, distribution or making available in any other form; or
c) merging, linking, as well as any restriction, degradation, erasure or destruction of information.

4.7 Record

Means any recorded information, regardless of form or medium, including:

a) Writing on any material.
b) Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored.
c) Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means.
d) Book, map, plan, graph or drawing.
e) Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

4.8 Filing System

Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

4.9 Unique Identifier
Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

4.10 De-Identify
This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

4.11 Re-Identify
In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

4.12 Consent
Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

4.13 Direct Marketing
Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
b) Requesting the data subject to make a donation of any kind for any reason.

4.14 Biometrics
Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

5. PURPOSE

This purpose of this policy is to protect **ASDSA**[AR2] from the compliance risks associated with the protection of personal information which includes:

a) Breaches of confidentiality. **ASDSA** could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
b) Failing to offer choice. All data subjects should be free to choose how and for what purpose **ASDSA** uses information relating to them.

c) Reputational damage. The professional body could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by **ASDSA**.

This policy confirms **ASDSA's** commitment to protecting the privacy rights of data subjects in the following manner:

a) Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
b) By cultivating a professional body with a culture that recognises privacy as a valuable human right.
c) By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
d) By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of **ASDSA**. and
e) By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of **ASDSA** and data subjects.
f) By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

6. PROFESSIONAL BODY SCOPE

This policy and its guiding principles applies to:

a) **ASDSA'S** management.
b) All branches, committees, business units and divisions of **ASDSA**
c) All Agent, volunteers and stakeholders.
d) All contractors, suppliers and other persons acting on behalf of **ASDSA**.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the professional body's PAIA Policy [AR3][SvdH4] as required by the Promotion of Access to Information Act (Act No 2 of 2000). The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or[AR5][SvdH6]
- where the personal information has been de-identified.

7. RIGHTS OF DATA SUBJECTS

Where appropriate, **ASDSA** will ensure that its members, designees and associates are made aware of the rights conferred upon them as data subjects. **ASDSA** will ensure that it gives effect to the following rights:

7.1 The Right to Access Personal Information

ASDSA recognises that a data subject has the right to establish whether **ASDSA** holds personal information related to him, her. This includes the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under **Annexure A.**

7.2 The Right to Have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his/her personal information must be corrected or deleted where **ASDSA** is no longer authorised to retain the personal information.

7.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his/her personal information. In such circumstances, **ASDSA** will give due consideration to the request and the requirements of POPIA. **ASDSA** may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

7.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his/her personal information for purposes of direct marketing by means of unsolicited electronic communications.

7.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his/her personal information. An example of a "POPI Complaint Form" can be found under **Annexure B.**

7.6 The Right to be Informed

The data subject has the right to be notified that his/her personal information is being collected by **ASDSA**. The data subject also has the right to be notified in any situation where **ASDSA** has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

8. GENERAL GUIDING PRINCIPLES

All Agents, volunteers and persons acting on behalf of **ASDSA** will at all times be subject to, and act in accordance with, the following guiding principles:

8.1 Accountability

Failing to comply with POPIA could potentially damage **ASDSA'S's** reputation or expose the professional body to a civil claim for damages. The protection of personal information is therefore everybody's responsibility. **ASDSA** will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, **ASDSA** will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

8.2 Processing Limitation

ASDSA will ensure that personal information under its control is processed:

a) in a lawful and non-excessive manner, and
b) only with the informed consent of the data subject, and
c) only for a specifically defined purpose.

ASDSA will inform the data subject of the reasons for collecting his/her personal information and obtain written consent prior to processing personal information. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, **ASDSA** will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

ASDSA will under no circumstances distribute or share personal information between separate legal entities, associated professional body's (such as other professional bodies or trade associations) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected. Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the professional body's business and be provided with the reasons for doing so.

An example of a "POPIA Notice and Consent Form" can be found under **Annexure C**.

8.3 Purpose Specification

All of **ASDSA's** business units and operations must be informed by the principle of transparency. **ASDSA** will process personal information only for specific, explicitly defined and legitimate reasons. **ASDSA** will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

8.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where **ASDSA** seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, **ASDSA** will first obtain additional consent from the data subject.

8.5 Information Quality

ASDSA will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the professional body will put into ensuring its accuracy.

Where personal information is collected or received from third parties, **ASDSA** will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

8.6 Open Communication

ASDSA will take reasonable steps to ensure that data subjects are notified that their personal information is being collected including the purpose for which it is being collected and processed.

ASDSA will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

a) Enquire whether the professional body holds related personal information, or
b) Request access to related personal information, or
c) Request the professional body to update or correct related personal information, or
d) Make a complaint concerning the processing of personal information.

8.7 Security Safeguards

ASDSA will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction. Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.[AR7][SvdH8]

ASDSA will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the professional body's IT network.

ASDSA will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals. All new agents will be required to sign employment contracts containing contractual terms for the use and storage of Agent, volunteer information.[AR9][SvdH10] Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the professional body is responsible. All existing agents and volunteers will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

ASDSA operators and third-party service providers will be required to enter into service level agreements with the professional body where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement. An example of "Agent, volunteer Consent and Confidentiality Clause" for inclusion in **ASDSA's** employment contracts can be found under **Annexure D**. An example of an "SLA Confidentiality Clause" for inclusion in **ASDSA's** service level agreements can be found under **Annexure E.**

8.8 Data Subject participation

A data subject may request the correction or deletion of his/her personal information held by the professional body. **ASDSA** will ensure that it provides a facility for data subjects who want to request the correction or deletion of their personal information. Where applicable, the professional body will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

9. INFORMATON OFFICERS

ASDSA will appoint an Information Officer [AR11][SvdH12]and where necessary, if required a Deputy Information Officer to assist the Information Officer. **ASDSA's** Information Officer is responsible for ensuring compliance with POPIA.

There are no legal requirements under POPIA for **ASDSA** to appoint an information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger professional body's.

Where no information officer is appointed, the head of **ASDSA** will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, **ASDSA** will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties. An example of an "Information Officer Appointment Letter" can be found under **Annexure F**.

10. SPECIFIC DUTIES AND RESPONSIBILITIES

10.1 The Executive Committee

ASDSA's executive committee [AR13][SvdH14]cannot delegate its accountability and is ultimately answerable for ensuring that the professional body meets its legal obligations in terms of POPIA. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals. The management body is responsible for ensuring that:

a) **ASDSA** appoints an Information Officer, and where necessary, a Deputy Information Officer.
b) All persons responsible for the processing of personal information on behalf of the professional body:
    a. are appropriately trained and supervised to do so,
    b. understand that they are contractually obligated to protect the personal information they come into contact with, and
    c. are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
c) Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
d) The scheduling of a periodic POPIA Audit [AR15][SvdH16]in order to accurately assess and review the ways in which **ASDSA** collects, holds, uses, shares, discloses, destroys and processes personal information.

10.2 Information Officer

ASDSA Information Officer is responsible for:

a. Taking steps to ensure **ASDSA** reasonable compliance with the provision of POPIA.
b. Keeping the governing body updated about the professional body's information protection responsibilities under POPIA. In the case of a security breach, the Information Officer must inform and advise the management body of their obligations pursuant to POPIA.
c. Continually analysing privacy regulations and aligning them with the professional body's personal information processing procedures. This will include reviewing **ASDSA's** information protection procedures and related policies.
d. Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
e. Ensuring that **ASDSA** makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the professional body. Maintaining a "contact us" facility on **ASDSA** website.
f. Approving any contracts entered into with operators, Agent, volunteers and other third parties which may have an impact on the personal information held by the professional body. This will include overseeing the amendment of **ASDSA's** employment contracts and other service level agreements.
g. Encouraging compliance with the conditions required for the lawful processing of personal information.

h. Ensuring that Agent, volunteers and other persons acting on behalf of **ASDSA** are fully aware of the risks associated with the processing of personal information and that they remain informed about **ASDSA** security controls.
i. Organising and overseeing the awareness training of Agent, volunteers and other individuals involved in the processing of personal information on behalf of **ASDSA**.
j. Addressing Agent, volunteers' POPIA related questions.
k. Addressing all POPIA related requests and complaints made by **ASDSA** data subjects.
l. Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

10.3 Chief Technical & Commercial Officer (Service provider)

ASDSA Chief Technical Officer [AR17][SvdH18] is responsible for:

a. Ensuring that **ASDSA** IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
b. Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
c. Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
d. Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
e. Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
f. Ensuring that personal information being transferred electronically is encrypted.
g. Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
h. Performing regular IT audits to ensure that the security of the professional body's hardware and software systems are functioning properly.
i. Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
j. Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the professional body's behalf.
k. Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the professional body's website, including those attached to communications such as **emails** and electronic newsletters.
l. Addressing any personal information protection queries from journalists or media outlets such as newspapers.
m. Where necessary, working with persons acting on behalf of the professional body to ensure that any outsourced marketing initiatives comply with POPIA.

10.5 Agents, Volunteers and other persons acting on behalf of ASDSA

Agents, volunteers and other persons acting on behalf of **ASDSA** will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain members, designees and other stakeholders.

Agents, volunteers and other stakeholders acting on behalf of **ASDSA** are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Agents, volunteers and other stakeholders acting on behalf of **ASDSA** may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within **ASDSA** or externally, any personal information, unless such information is already officially known or the disclosure is necessary in order for the agents, volunteers or person to perform his or her duties.

Agents, volunteers and other persons acting on behalf of **ASDSA** must request assistance from their committee chairperson or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information. Agents, volunteers and other persons acting on behalf of **ASDSA** will only process personal information where:

a. The data subject, or a competent person where the data subject is a child, consents to the processing; or
b. The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
c. The processing complies with an obligation imposed by law on the responsible party; or
d. The processing protects a legitimate interest of the data subject; or
e. The processing is necessary for pursuing the legitimate interests of the professional body or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

a. Clearly understands why and for what purpose his/her personal information is being collected; and
b. Has granted the professional body with explicit written or verbally recorded consent to process his/her personal information.

Agents, volunteers and other persons acting on behalf of **ASDSA** will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his/her personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, **ASDSA** will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

a. the personal information has been made public, or
b. where valid consent has been given to a third party, or
c. the information is necessary for effective law enforcement.

Agents, volunteers and other persons acting on behalf of **ASDSA** will under no circumstances:

a. Process or have access to personal information where such processing or access is not a requirement to perform their respective professional body tasks or duties.
b. Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the professional body's central database or a dedicated server[AR19][SvdH20] and or alternative secure platforms and systems will be made available to secure the data of the members, designees and stakeholders.
c. Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant chairperson or the Information Officer.
d. Transfer personal information outside of South Africa without the express permission from the Information Officer.

Agents, volunteers and other persons acting on behalf of **ASDSA** are responsible for:

a. Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
b. Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
c. Ensuring that personal information is encrypted prior to sending or sharing the information electronically. [AR21][SvdH22] The Systems and Information Officer will assist Agents, volunteers, committee chairs and where required, other persons acting on behalf of the professional body, with the sending or sharing of personal information to or with authorised external persons.
d. Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
e. Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
f. Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

g. Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. In a locked drawer of a filing cabinet or lockable filing cabinet.
h. Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them.
i. Taking reasonable steps to ensure that personal information is kept accurate and up to date. Confirming a data subject's contact details when the members, designees or stakeholders communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant chairperson or the Information Officer to update the information accordingly.
j. Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant Chairperson or the Information Officer to delete or dispose of the personal information in the appropriate manner.
k. Undergoing POPIA Awareness training from time to time.

Where an agent, volunteer, or a person acting on behalf of **ASDSA**, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

11. POPIA AUDIT [AR23][SvdH24]

ASDSA Information Officer will schedule periodic POPIA Audits. The purpose of a POPIA audit is to:

a. Identify the processes used to collect, record, store, disseminate and destroy personal information.
b. Determine the flow of personal information throughout **ASDSA**. Various business units, divisions, branches and other associated professional body's.
c. Redefine the purpose for gathering and processing personal information.
d. Ensure that the processing parameters are still adequately limited.
e. Ensure that new data subjects are made aware of the processing of their personal information.
f. Re-establish the rationale for any further processing where information is received via a third party.
g. Verify the quality and security of personal information.
h. Monitor the extend of compliance with POPIA and this policy.
i. Monitor the effectiveness of internal controls established to manage the professional body's POPI related compliance risk.

In performing the POPIA Audit, Information Officers will liaise with executive Committee member in order to identify areas within in **ASDSA's** operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from executive Committee member and the professional body's governing body in performing their duties.

12. REQUEST TO ACCESS PERSONAL INFORMATION

Data subjects have the right to:

a. Request what personal information the professional body holds about them and why.
b. Request access to their personal information.
c. Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a **"Personal Information Request Form**". Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the professional body's PAIA Policy. The Information Officer will process all requests within a reasonable time.

13. POPIA COMPLIANT PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. **ASDSA** takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

a. POPIA complaints must be submitted to the professional body in writing. Where so required, the Information Officer will provide the data subject with a "POPIA **Complaint Form**".
b. Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
c. The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
d. The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
e. The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the professional body's data subjects.
f. Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information

Officer will consult with the professional body's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

g. The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the professional body's governing body within 7 working days of receipt of the complaint. In all instances, the professional body will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
h. The Information Officer's response to the data subject may comprise any of the Following:
    i. A suggested remedy for the complaint,
    ii. A dismissal of the complaint and the reasons as to why it was dismissed, An apology (if applicable) and any disciplinary action that has been taken against any Agent, volunteers involved.
    iii. Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.

The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.

14. DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA infringement investigation has been finalised, **ASDSA** may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any Agent, volunteer reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, **ASDSA** will undertake to provide further awareness training to the Agent, volunteer.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which **ASDSA** may summarily dismiss the Agent, volunteer or terminate the Service Level Agreement where this function has been outsourced. Disciplinary procedures will commence where there is sufficient evidence to support an Agent, volunteer's gross negligence.

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

a. A recommendation to commence with disciplinary action.
b. A referral to appropriate law enforcement agencies for criminal investigation.
c. Recovery of funds and assets in order to limit any prejudice or damages caused.

15. LEGISLATIVE FRAMEWORK

ASDSA manages its legislative framework within its defined regulatory and legislative framework as defined within its Compliance Risk Management Framework.

16. REFERENCES

Compliance files, policies and manual are maintained by the compliance function. These include:

a. Compliance Risk Management Framework
b. Compliance Manual including all Policies, Processes and Procedures

Requests for any compliance information or documentation to be submitted.

17. APPROVAL STRUCTURES

Approval required by Director and Executive Management.

All Policy and procedures are drafted and sent to exco and then ratified and updated into our QMS. All major policies and procedures that require board approval is first circulated to the board directors for approval and then ratification and adoption.

INFORMATION OFFICER

Name **Contact number** **Email Address:**	Sharon van den Heever
	082 775 1221
	exco@asdsa.org.za

DIRECTOR 1

Name **Contact number** **Email Address:**	Andy Reinecke

DIRECTOR 2

Name **Contact number** **Email Address:**	Maryna Ritter

18. POLICY SPONSOR

Head of Legal Risk and Compliance

DIRECTOR 1

Name **Contact number** **Email Address:**	Sharon van den Heever
	082 775 1221
	exco@asdsa.org.za

DIRECTOR 2

Name **Contact number** **Email Address:**	Andy Reinecke

19. CONTACT PERSON

The following person may be contacted in relation to this policy

DIRECTOR 1

Name **Contact number** **Email Address:**	Sharon van den Heever
	082 775 1221
	exco@asdsa.org,za

DIRECTOR 2

Name **Contact number** **Email Address:**	Andy Reinecke

ANNEXURE A:

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer:

Name **Contact number** **Email Address:**	

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject

Name & surname **Identity Number:** **Postal Address:** **Contact Number:** **Email Address:**	

B. Request

I request the professional body to:

(a) Inform me whether it holds any of my personal information
(b) Provide me with a record or description of my personal information
(c) Correct or update my personal information
(d) Destroy or delete a record of my personal information

C. Instructions

Signature
Date

ANNEXURE B:

POPIA COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit your complaint to the Information Officer:

Name **Contact Number** **Email Address:**	

Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information **Regulator.**

The Information Regulator:
Physical Address:
Email:
Website:

A. Particulars of Complainant

Name & Surname **Identity Number:** **Postal Address:** **Contact Number:** **Email Address:**	

B. Details of Complaint

C. Desired Outcome

Signature:
Date

ANNEXURE C:

POPIA NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's Contact Details

Name **Contact Number** **Email Address:**	

Purpose for Processing your Information

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit reference searches
- To issue, administer and manage your insurance policies
- To process insurance claims and to take recovery action
- To notify you of new products or developments that may be of interest to
- you to confirm, verify and update your details
- To comply with any legal and regulatory requirements

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information and your banking details.

Consent to Disclose and Share your Information

We may need to share your information to provide advice, reports, analyses, products or services that you have requested.

Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

I hereby authorise and consent to the professional body sharing my personal information with the following persons:

Name & Surname
Signature
Date

ANNEXURE D:

AGENTS, VOLUNTEERS CONSENT AND CONFIDENTIALITY CLAUSE

'Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

"POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

The professional body undertakes to process the PI of the Agent, volunteer only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the professional body's relevant policy available to the Agent, volunteer on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as a professional body and within the framework of the professional body and as required by South African law.

The Agent, volunteer acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the professional body. The Agent, volunteer therefore irrevocably and unconditionally agrees: That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the professional body's discharge of its obligations and to perform its functions as a professional body.

That he/she consents and authorises the professional body to undertake the collection, processing and further processing of the Agent, volunteer's PI by the professional body for the purposes of securing and further facilitating the Agent, volunteer's SLA with the professional body. Without derogating from the generality of the afore stated, the Agent, volunteer consents to the professional body's collection and processing of PI pursuant to any of the professional body's Internet, Email and Interception policies in place insofar as PI of the Agent, volunteer is contained in relevant electronic communications.

To make available to the professional body all necessary PI required by the professional body for the purpose of securing and further facilitating the Agent, volunteer's employment with the professional body. To absolve the professional body from any liability in terms of POPIA for failing to obtain the Agent, volunteer's consent or to notify the Agent, volunteer of the reason for the processing of any of the Agent, volunteer's PI. To the disclosure of his/her PI by the professional body to any third party, where the professional body has a legal or contractual duty to disclose such. The Agent, volunteer further agrees to the disclosure of his/her PI for any reason enabling the professional body to carry out or to comply with any business obligation the professional body may have or to pursue a legitimate

interest of the professional body in order for the professional body to perform its business on a day-to-day basis.

The Agent, volunteer authorises the professional body to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the professional body within the international community. The professional body undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard. The Agent, volunteer acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain agents, volunteers, suppliers and other Stakeholders. The agents and volunteers will treat personal information as a confidential business asset and agrees to respect the privacy of Members, suppliers and other Agent, volunteers.

To the extent that he/she is exposed to or insofar as PI of other Agent, volunteers or third parties are disclosed to him/her, the Agent, volunteer hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or Agent, volunteers. Agent, volunteers may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the professional body or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the Agent, volunteer or person to perform his or her duties on behalf of the professional body.

ANNEXURE E:

SLA CONFIDENTIALITY CLAUSE

"Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

"POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to PI and other information that may be classified or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.

The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its Agent, volunteers, its contractors or other authorised individuals comes into contact with pursuant to this agreement.

Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

ANNEXURE F:

INFORMATION OFFICER APPOINTMENT LETTER

Herewith and with immediate effect appoint you as the Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing. You are entrusted with the following responsibilities:

a. Taking steps to ensure the professional body's reasonable compliance with the provision of POPIA.
b. Keeping the governing body updated about the professional body's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
c. Continually analysing privacy regulations and aligning them with the professional body's personal information processing procedures. This will include reviewing the professional body's information protection procedures and related policies.
d. Ensuring that POPI Audits are scheduled and conducted on a regular basis.
e. Ensuring that the professional body makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the professional body, to do so. For instance, maintaining a "contact us" facility on the professional body's website.
f. Approving any contracts entered into with operators, Agent, volunteers and other third parties which may have an impact on the personal information held by the professional body. This will include overseeing the amendment of the professional body's employment contracts and other service level agreements.
g. Encouraging compliance with the conditions required for the lawful processing of personal information.
h. Ensuring that Agent, volunteers and other persons acting on behalf of the professional body are fully aware of the risks associated with the processing of personal information and that they remain informed about the professional body's security controls.
i. Organising and overseeing the awareness training of Agent, volunteers and other individuals involved in the processing of personal information on behalf of the professional body.
j. Addressing Agent, volunteers' POPIA related questions.
k. Addressing all POPIA related requests and complaints made by the professional body's data subjects.

Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

I hereby accept the appointment as Information Officer
Name & Surname **Signature** **Date**