

**WEBSITE PRIVACY POLICY OF SASSDA**

JUNE 2021

**TABLE OF CONTENTS**

1. PURPOSE OF POLICY
2. EXPLANATION OF TERMS
3. APPLICATION
4. LEGAL FRAMEWORK
5. OTHER
6. INFORMATION OFFICER
7. PERSONAL INFORMATION
8. INFORMATION NOT SUBJECT TO THIS POLICY
9. DATA SUBJECTS' RIGHTS
10. COLLECTION OF PERSONAL INFORMATION
11. ACCESS TO AND USE OF PERSONAL INFORMATION
12. PRE-AUTHORISATION BY THE INFORMATION REGULATOR
13. CONSENT
14. FURTHER PROCESSING
15. SHARING AND DISCLOSURE OF PERSONAL INFORMATION
16. NOTIFICATIONS TO DATA SUBJECTS
17. SECURING PERSONAL INFORMATION
18. PROCESSING OF INFORMATION BY THIRD PARTIES
19. RETENTION AND STORAGE OF RECORDS
20. ACCESS TO RECORDS BY DATA SUBJECTS
21. ENSURING ACCURACY OF PERSONAL INFORMATION
22. RESTRICTION OF PROCESSING
23. SENDING INFORMATION ACROSS THE BORDERS OF THE REPUBLIC OF SOUTH AFRICA ("RSA")
24. HISTORICAL, STATISTICAL AND RESEARCH PURPOSES
25. MARKETING ACTIVITIES
26. PROFILING
27. INFORMATION REGULATOR
28. SECURITY COMPROMISES
29. COMPLAINTS
30. VERIFICATION OF COMPLIANCE WITH POLICY AND AUDIT
31. NON-COMPLIANCE WITH THIS POLICY
32. IMPLEMENTATION OF THIS POLICY
33. EFFECTIVE DATE OF POLICY
34. POLICY REVISION

Association incorporated under Section 21 – Reg. No. 2003/022992/08  
1<sup>st</sup> Floor, Palm Grove, Houghton Estate Office Park, 2 Osborn Road, Houghton, 2198  
P O Box 4479, Rivonia, 2128  
Tel: +27 11 883 0119 Email: [info@sassda.co.za](mailto:info@sassda.co.za) Website: [www.sassda.co.za](http://www.sassda.co.za)

Directors: LD Griesel (Chairperson) GAR Whitty (Vice-Chairperson) MA Basson (Acting Executive Director)  
CD Cammell MJ Campbell BH Maguire JM Naudé NB Ntshangase Veldsman BA Visser C Wilson

**Stainless Steel. It's Simply Brilliant.**

## 1. PURPOSE OF POLICY

Sassda shares information to and about member companies on the Associations website. Your privacy is very important and Sassda is committed to protecting your and your companies personal and sensitive information and the privacy thereof. This Policy will explain the scope of information collected, stored, and used on the website. The Personal Information Management Policy of Sassda describes how Sassda collects, communicates, and use any personal information that you submit to us or through which we obtain upon you accessing the Website. This Policy governs, in conjunction and in cooperation, with other website Terms and Conditions or any other documentation and/ or rulings published or still to be published.

## 2. EXPLANATION OF TERMS

- 2.1 **“Website”** refers to the Sassda website: [www.sassda.co.za](http://www.sassda.co.za), provides profile, signature and industry related updates and information to enable to inform members and stakeholders themselves of the training programmes and the industry support in which Sassda offer.
- 2.2 **“Data subject”** refers to the member to whom the personal information relates. Data subjects in the association setting include member companies, individuals working for member companies or persons who may act on their behalf, and any other person or entity of which the association has personal information in its possession or under its control.
- 2.2 **“PAIA”** means the Promotion of Access to Information Act 2 of 2000 and the Regulations made in terms thereof.
- 2.3 **“Association”** means the Southern African Stainless Steel Development Association - SASSDA
- 2.4 **“Personal Information”** refers to information relating to identifiable, living, natural persons as well as identifiable, existing juristic persons, and includes, but is not limited to:
- (a) information relating to the race, gender, 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 assignment to the person;

- (d) the personal opinions, views, or preferences of the person;
- (e) 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;
- (f) the views or opinions of another individual about the person; and
- (g) 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.

The personal information of living natural persons (i.e., human beings) and existing juristic persons (e.g., companies) is protected under POPIA.

2.5 **“POPIA”** means the Protection of Personal Information Act 4 of 2013 and the Regulations made in terms thereof.

2.6 **“Processing”** means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including –

- 2.6.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- 2.6.2 dissemination by means of transmission, distribution or making available in any other form; or
- 2.6.3 merging, linking, as well as restriction, degradation, erasure, or destruction of information.

For purposes of this Policy, ‘processing’ includes any activity that can be undertaken in respect of personal information.

2.7 **“Public record”** means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether it was created by that public body.

2.8 **“Record”** means any recorded information:

2.8.1 regardless of form or medium, including any of the following:

- 2.8.1.1 writing on any material.;
- 2.8.1.2 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;

2.8.1.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.8.1.4 book, map, plan, graph, or drawing;

2.8.1.5 photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.

2.8.2 in the possession or under the control of a responsible party;

2.8.3 whether it was created by a responsible party; and

2.8.4 regardless of when it came into existence.

2.9 **“SOP”** refers to a Standard Operating Procedure of the association.

2.10 **“Unique identifier”** refers to 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.

### **3. APPLICATION**

This Policy applies to the Association, its directors, partners, employees (including temporary and part-time employees), contractors, who have access to or process personal information. This includes any activity or operation, whether automated or not, concerning personal information, such as to collect, use, disseminate, store, or disclose that information, for and on behalf of the Association. The Terms and Conditions of use regulate access to and use of the website, member information and other relevant information contained within the Website, any profile, information, and signature used, downloaded, uploaded distributed and shared by you and the uploading of any content and material (including text, files, images, and photographs) on the Website.

### **4. LEGAL FRAMEWORK**

4.1 The following laws and their Regulations govern, amongst others, the processing and confidentiality of personal information and must be considered in conjunction with this Policy:

4.1.1 Constitution of South Africa (Act 108 of 1996);

4.1.2 Electronic Communications and Transactions Act 25 of 2002;

4.1.3 PAIA; and

4.1.4 POPIA.

4.2 The Ethical Rules and other relevant policies and directives of the Association and country.

4.3 If any conflict occurs between a provision of this Policy and the law, the law prevails.

## 5. OTHER POLICIES

This Policy must be considered in conjunction with other policies and SOPs related to the processing of personal information, such as the Privacy Policy, Record Retention Policy, Information Technology (IT) Policy and the Website Terms and Conditions of the Association.

## 6. INFORMATION OFFICER

The Information Officer of the Association is:

<b>Name:</b>	Mrs. Francis le Roux
<b>Position:</b>	Head: Administration
<b>Contact telephone number:</b>	Tel: +27 11 883 0119   Cell: +27 72 200 8322
<b>E-mail address</b>	Francis@sassda.co.za

If any uncertainty exists about the application of this Policy or if there is any query or question in relation to the processing of personal information in the performance of duties or the discharge of functions, the Information Officer must be contacted for support and guidance.

## 7. PERSONAL INFORMATION

7.1 For purposes of this Policy, 'personal information' includes all personal information of any data subject in the possession or under the control of the Association, including personal information of deceased persons, but not information of juristic persons that no longer exist.

7.2 Personal information must be handled with utmost care to secure and maintain the confidentiality and integrity of that information as required in terms of the law.

7.3 An obligation of confidentiality must be imposed on employees through their employment or other agreements or another appropriate mechanism.

## **8. INFORMATION NOT SUBJECT TO THIS POLICY**

Information, from which the identity of data subjects cannot be determined, such as trend analyses and aggregate reporting, is not subject to this Policy. In legal terms this refers to de-identified information that cannot be re-identified.

## **9. DATA SUBJECTS' RIGHTS**

9.1 Data subjects have the following rights:

- 9.1.1 to have their personal information processed in accordance with the conditions for the lawful processing of personal information as set out in POPIA;
- 9.1.2 to be notified that their personal information is being collected;
- 9.1.3 to be notified that their personal information has been accessed or acquired by an unauthorised person;
- 9.1.4 to establish whether the Association holds personal information of them and to request access to that information;
- 9.1.5 to request, where necessary, the correction, destruction, or deletion of their personal information;
- 9.1.6 to object, on reasonable grounds to the processing of their personal information as provided for in POPIA;
- 9.1.7 to object to the processing of their personal information for purposes of direct marketing;
- 9.1.8 not to have their personal information processed for purposes of direct marketing by means of unsolicited electronic communications, except as provided for in POPIA;
- 9.1.9 not to be subject to a decision, which is based solely on the automated processing of their personal information, and which provides profiles of them, except as provided for in POPIA; and
- 9.1.10 to submit a complaint to the Information Regulator or institute civil proceedings regarding the alleged interference with the protection of their personal information.

## **10. COLLECTION OF PERSONAL INFORMATION**

- 10.1 Personal information may only be collected, if it is required by the Association for lawful purposes related to its function and activities and as provided for in relevant legislation. No more information than what is necessary must be collected.
- 10.2 The purposes for which personal information is collected by the Association must, amongst others, be communicated to the affected data subjects, as may be necessary from time to time.
- 10.3 Personal information must as far as possible be collected directly from the person to whom it relates.
- 10.4 Personal information may be collected from other sources in the following circumstances:
  - 10.4.1 If the person to whom the information relates has provided written consent.
  - 10.4.2 The information is contained in a public record.
  - 10.4.3 The information has deliberately been made public by the data subject.
  - 10.4.4 It will not prejudice a legitimate interest of the data subject.
  - 10.4.5 To comply with an obligation imposed by law.
  - 10.4.6 It is necessary to maintain the legitimate interests of the Association or of a third party to whom the information is supplied.
  - 10.4.7 Obtaining the information from the data subject is not reasonably practicable in the circumstances.
  - 10.4.8 Obtaining the information from the data subject will prejudice a lawful purpose of the collection; or
  - 10.4.9 It is necessary for proceedings in a court or tribunal.

What constitutes a 'legitimate interest' must be determined with reference to the facts of the situation. The Information Officer must be requested for guidance in this regard.

## **11. ACCESS TO AND USE OF PERSONAL INFORMATION**

- 11.1 Employees may only have access to personal information if it is reasonably required for the performance of their duties and functions. Employees must not attempt to gain access beyond their access privileges and may not bypass security controls without the approval of the Information Officer.

- 11.2 Access to the accounting records or other commercially sensitive information of the Association is subject to approval by the Managing Director and the Information Officer.
- 11.3 Third parties (such as service providers and consultants) may only be provided with access to personal information if it is reasonably required for the performance of their functions with approval from the Managing Director and the Information Officer. Their use must be monitored by the Information Officer or another designated person.
- 11.4 Personal information may not be used in a manner that breaches the privacy of any person.
- 11.5 Personal information may only be used for lawful purposes related to the business of the Association or as otherwise provided for in legislation or with the written consent of the member or other data subject. Personal information to which an employee gained access as part of discharging his/her functions at the Association may not be used by the employee for any other purpose than that for which the information was provided or obtained.
- 11.6 Personal information, other than special personal information, may be processed in the following circumstances:
  - 11.6.1 With written consent of the data subject.
  - 11.6.2 For the conclusion or performance of a contract to which the data subject is party,
  - 11.6.3 For compliance with an obligation imposed by law.
  - 11.6.4 For the protection of a legitimate interest of the data subject unless the data subject objects on reasonable grounds on the prescribed form; or
  - 11.6.5 For the pursuit of the legitimate interests of the Association or of a third party to whom the information is supplied unless the data subject objects on reasonable grounds on the prescribed form.

What constitutes a 'legitimate interest' as contemplated above must be determined with reference to the facts of the situation. The Information Officer must be requested for guidance in this regard.

- 11.7 Race-related information may be processed with consent of the member. The Association may process race-related information of employees to comply with obligations imposed by law, such as the Employment Equity Act 55 of 1998. The



processing of race-related information of other data subjects requires their written consent unless it is permitted by law.

- 11.8 There could be circumstances when personal information may only be lawfully used for certain restricted purposes, which are defined in legislation. This will, for example, occur when the accuracy of the information in the possession or under the control of the Association is contested by a data subject.
- 11.9 Employees, who have resigned, terminated their contracts with the Association, or have been dismissed, must be assessed as to their continuing need for access to personal information in the possession or under the control of the Association. Access to such information may only continue with permission of the Managing Director and the Information Officer.
- 11.10 Practitioners and employees who are subject to disciplinary action or who face criminal charges, may only have access to personal information with the express permission of the Managing Director and the Information Officer.

## **12. PRE-AUTHORISATION BY THE INFORMATION REGULATOR**

- 12.1 The Information Officer must obtain pre-authorization from the Information Regulator as set out in POPIA before any of the following processing takes place:
  - 12.1.1 Processing of unique identifiers of data subjects (e.g., file numbers) for a purpose other than the purpose for which the identifier was intended at collection and with the aim of linking that information with information processed by other responsible parties.
  - 12.1.2 Processing of information for the purposes of credit reporting.
  - 12.1.3 Processing of other types of information as specified by the Information Regulator.
- 12.2 No processing of the personal information set out in paragraph 12.1 may occur until the Information Officer advises otherwise with due consideration of the provisions of POPIA.
- 12.3 If any of the abovementioned processing activities occur on 1 July 2020, they can proceed and must only be suspended when the Information Regulator determines otherwise by notice in the Government Gazette. The Information Officer must, however, still notify the processing activities to the Information Regulator as prescribed.

### **13. CONSENT**

- 13.1 Consent provided by any data subject must be in writing and must, as far as possible, occur on consent forms designed by the Association for this purpose or otherwise on forms as prescribed by law.
- 13.2 Consent must be comprehensive and cover all reasonable processing activities of the Association.
- 13.3 Where a designated individual at a member company cannot independently consent, a competent person, i.e., a person authorized in terms of the law may provide the necessary consent.
- 13.4 Consent may be withdrawn at any time. Such withdrawal must be respected by employees. All processing activities conducted before withdrawal of the consent remain valid and lawful. Any processing activities conducted after withdrawal of the consent must be authorized in terms of the law.
- 13.5 The Information Officer must in conjunction with the IT support function design a mechanism to record consent and the withdrawal of consent by data subjects, which information must be available to practitioners and authorised employees.

### **14. FURTHER PROCESSING**

- 14.1 If the Association has collected personal information for a specific purpose and would like to process it further (e.g., for research purposes, for collection of an outstanding amount, etc.) such further processing must be compatible with the purpose for which the information was originally collected.
- 14.2 The Information Officer must determine whether the further processing of that information is compatible with the purpose of collection with reference to the following criteria:
  - 14.2.1 the relationship between the purpose of the further processing and the purpose for which the information has been collected;
  - 14.2.2 the nature of the information;
  - 14.2.3 the consequences of such further processing for the data subject;
  - 14.2.4 the way the information has been collected; and
  - 14.2.5 any contractual rights and obligations between the parties.
- 14.3 Any intended further processing of personal information must be reported to the Information Officer, who must confirm whether such processing may occur.

## **15. SHARING AND DISCLOSURE OF PERSONAL INFORMATION**

- 15.1 Personal information may only be shared with or disclosed to other parties to fulfil the purposes identified at the time of the collection of that information, or for a purpose reasonably related to those purposes (e.g., sharing with the accountant for billing purposes), provided that these parties require the information reasonably and lawfully for the performance of their duties or functions.
- 15.2 Other disclosures of personal information require the written consent of the data subject unless such disclosures are permitted in terms of the law (e.g., reporting of notifiable conditions).
- 15.3 The Association's database with membership and other personal information may not be shared with or sold to other persons unless all the affected data subjects have provided consent.
- 15.4 Sharing of Association-related information with statutory bodies must be signed off by the Information Officer. Identifiable information of persons may not be included in such information unless consent has been provided by the relevant persons or it is permitted in terms of the law.
- 15.5 No personal information of any data subject may be shared on social media without the express permission of the Information Officer.
- 15.6 Association in the place and manner as determined by the Information Officer and must include the nature of the information disclosed and the recipient's identity.

## **16. NOTIFICATIONS TO DATA SUBJECTS**

- 16.1 When the Association collects personal information, it must communicate certain information to the relevant data subjects. This will assist to make the processing of that information reasonable.
- 16.2 The following information must be communicated:
  - 16.2.1 the information being collected;
  - 16.2.2 the source of collection, if not collected from the data subject;
  - 16.2.3 the name and address of the Association;
  - 16.2.4 the purpose for which the information is collected;
  - 16.2.5 whether the supply of the information by the data subject is voluntary or mandatory;

- 16.2.6 the consequences if the information is not provided;
  - 16.2.7 any law requiring or authorising the collection;
  - 16.2.8 whether the Association intends to transfer the information to another country and the level of protection afforded to that information by that country;
  - 16.2.9 the recipient or category of recipients of the information;
  - 16.2.10 the nature of the information;
  - 16.2.11 the data subject has a right to access and request rectification of the information;
  - 16.2.12 the right of the data subject to object to the processing of the information as contemplated in POPIA; and
  - 16.2.13 the right of the data subject to lodge a complaint with the Information Regulator and the Regulator's contact details.
- 16.3 The information listed in paragraph 17.2 must only be communicated once to the data subject provided that any subsequent information collected is of the same kind and the purpose of collection remains the same.
- 16.4 The information listed in paragraph 17.2 must be communicated as follows:
- 16.4.1 When information is collected from the data subject: before collection unless the data subject is aware of this information.
  - 16.4.2 When information is collected from other sources: before collection or as soon as reasonably practicable after collection.
- 16.5 The information listed in paragraph 17.2 does not have to be communicated in the following circumstances:
- 16.5.1 the data subject or competent person consents in writing;
  - 16.5.2 there will not be prejudice to a legitimate interest of the data subject.;
  - 16.5.3 if it is necessary to comply with an obligation imposed by law;
  - 16.5.4 if it is necessary for proceedings in a court or tribunal;
  - 16.5.5 communication of the information will prejudice a lawful purpose of the collection;

- 16.5.6 communication of the information is not reasonably practicable in the circumstances;
  - 16.5.7 the information will not be used in a form that will identify the data subject; or
  - 16.5.8 the information will be used for historical, statistical or research purposes.
- 16.6 The Association will use various mechanisms to communicate the specified information, as determined by the Information Officer from time to time and required in the circumstances, such as its Privacy Policy, information forms, employment contracts and relevant policies.

## **17. SECURING PERSONAL INFORMATION**

- 17.1 The Association is committed to ensure the confidentiality and integrity of the personal information in its possession or under its control to protect such information from unauthorized access, collection, use, disclosure, dissemination, copying, modification, storage, or disposal.
- 17.2 The Association's IT Policy / SOP governs the use and access of information on or through the Association's IT infrastructure, portable computers, smart phones, and other handheld devices and includes directives related to the downloading of programmes, applications and information from the Internet, anti-virus software, as well as good practice related to suspicious e-mails and related matters. This Policy / SOP is integral to and must be read with this Policy.
- 17.3 The Information Officer must on a regular basis conduct a risk assessment in respect of the personal information in the possession or under the control of the Association. This includes:
  - 17.3.1 the identification of all reasonably foreseeable internal and external risks to the personal information;
  - 17.3.2 the establishment and maintenance of appropriate safeguards against the risks identified;
  - 17.3.3 the regular verification that the safeguards have been effectively implemented; and
  - 17.3.4 ensuring that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

- 17.4 The following security measures must be followed to ensure that the personal information is appropriately protected:
- 17.4.1 Each interface that gives an employee access to personal information contained in any record in the possession or under the control of the Association, including print-outs of electronic records, must be considered confidential and reasonable steps must be taken to protect these records from unauthorised access.
  - 17.4.2 Hard copy records and printouts of electronic records containing personal information must not be left unattended on desks, printers or photocopiers or similar equipment, or in offices during employees' absence from their work areas or offices, even for brief periods, or in areas (e.g., reception) where unauthorised persons may access them. They must be securely stored in a lockable drawer, cabinet or safe with the keys removed.
  - 17.4.3 Matters involving personal information should never be discussed in public areas. Telephone discussions and interviews with persons, which involve the disclosure of personal information about them or another person, must be conducted in areas where confidentiality can be maintained.
  - 17.4.4 Individual offices must be locked outside of business hours.
  - 17.4.5 Employees must only use secure routes to send personal information and always mark the information as confidential. The risks and consequences of unauthorised or accidental release of personal information must be assessed when transmitting information by e-mail or any other means.
  - 17.4.6 Employees must only obtain and keep the minimum amount of personal information necessary to perform their duties or functions.
  - 17.4.7 Employees must only copy and/or share records containing personal information with other persons when it is necessary to perform their duties or functions and sharing of personal information may only occur with authorised persons as set out in this Policy, a relevant SOP or in accordance with the law.
  - 17.4.8 If practicable, documents must be converted into an electronic format and be stored on an encrypted device.
  - 17.4.9 Record storage areas must be locked when not in use.
  - 17.4.10 Access to server rooms and storage areas for electronic records must be managed with key card access.

17.4.11 Documents, including printouts of records, containing personal information may only be destroyed through the secure mechanisms provided by the Association (such as secure shredding services). These documents may not be disposed of at home, while traveling or by placing them in a dustbin.

17.5 Removing hard copy documents from the Association:

17.5.1 Employees may not remove hard copy documents containing personal information from the Association without the permission and knowledge of the Information Officer.

17.5.2 The Information Officer must monitor and log their removal and return, including the following, in a written record:

17.5.2.1 the type and format of the documents;

17.5.2.2 the personal information included in those documents;

17.5.2.3 the purpose for which the documents are being removed;

17.5.2.4 the period for which the documents are expected to be out of the office; and

17.5.2.5 when the documents have been returned.

17.5.3 Only the documents necessary to perform a duty or function must be removed.

17.5.4 The Information Officer must report any missing documents to the Managing Director within 24 hours of becoming aware thereof. This requirement is essential for the Association to investigate any potential loss of personal information.

17.5.5 Any authorised person, who removes documents containing personal information from the Association, must take reasonable and practicable steps to protect the documents from unauthorised disclosure or damage. For example, the documents must not be left unattended, including in bags at airports, in locked but empty cars or in any other unattended location, but must where possible, be kept in the personal possession of the authorised person.

17.6 The Association must continually review and update its security policies and controls as technology changes to ensure ongoing personal information security.

## **18. PROCESSING OF INFORMATION BY THIRD PARTIES**

If any person or entity processes personal information of any data subject on behalf of the Association, written agreements must be entered into with the relevant person or entity, which contains, amongst others, the information prescribed in POPIA and ensures that the Association is protected against any claim, which may arise if a security breach occurs.

## **19. RETENTION AND STORAGE OF RECORDS**

19.1 The Association must retain and store records containing personal information as provided for in the law. Personal information may only be deleted from records and records containing personal information may only be destroyed in accordance with this Policy.

19.2 In general, records with personal information must be retained for as long as they are required for lawful purposes related to the business of the Association. Records containing personal information that have been used to make decisions about persons must be retained for such periods that would allow those persons to request access to them.

## **20. ACCESS TO RECORDS BY DATA SUBJECTS**

20.1 A data subject has a right of access to his/her/its personal information in the possession or under the control of the Association subject to the provisions of PAIA, which allows the Association to refuse access to records or information in certain circumstances, for example, when it relates to an unreasonable disclosure of information of a person.

20.2 A fee is applicable to obtain access to certain types of personal information and records.

20.3 Requests for access to personal information or records in the possession of the Association, including the identities of persons / entities to whom the information has been disclosed, must be made on the prescribed form and after payment of the prescribed fee to the Information Officer, and must provide sufficient detail to identify the personal information or records being sought.

20.4 If a request for access is refused in full or in part, the Information Officer must advise the person requesting the access in writing of the reason(s) for refusal.

20.5 If access to information is granted to a data subject, he/she/it must be advised of his/her/its right to request a correction of that information as provided in POPIA.



## **21. ENSURING ACCURACY OF PERSONAL INFORMATION**

- 21.1 When personal information is collected, used or stored, reasonable efforts must be made to ensure that the information is accurate and complete, especially where the information may be used to make a decision about a member.
- 21.2 Persons in respect of whom the Association has personal information in its possession or under its control may request corrections to their information to ensure accuracy and completeness on the prescribed form.
- 21.3 Authorised employees may update or correct the contact details, when necessary. Other corrections of personal information and requests to delete information must be requested in writing by the members and other data subjects from the Information Officer on the prescribed form, providing sufficient detail to identify the relevant personal information and the correction or deletion required.
- 21.4 If any personal information is inaccurate or incomplete, the Information Officer must ensure that the information is corrected as required by legislation. The Information Officer must ensure that the corrected information is provided to all persons and entities to whom the information has been previously disclosed (e.g., funders), if the amended information will affect any decision made based on that information.
- 21.5 When the accuracy of the personal information in the possession or under the control
- 21.6 the reason for not performing the requested correction or deletion as required in terms of POPIA, if requested by the data subject.
- 21.7 An audit trail must be logged of all corrections made to electronic records or attempts to alter electronic records and their metadata.

## **22. RESTRICTION OF PROCESSING**

- 22.1 The processing of personal information by the Association must be restricted in the following circumstances:
  - 22.1.1 accuracy of the information is contested by the data subject;
  - 22.1.2 the information is no longer needed by the Association but is maintained for proof;
  - 22.1.3 processing is unlawful, and the data subject requests restriction of use instead of destruction or deletion of that information; or
  - 22.1.4 the data subject requests that the information must be transmitted into another automated processing system.

22.2 In the above circumstances, the information must be clearly identified as “restricted use” by the Information Officer in conjunction with the IT support function, and until the restriction is lifted, the Association may only:

22.2.1 store the information;

22.2.2 use the information for purposes of proof;

22.2.3 process the information with consent of the data subject;

22.2.4 process the information for the protection of the rights of another person;  
or

22.2.5 process the information in the public interest.

22.3 The Association must inform the data subject before the restriction is lifted.

### **23. SENDING INFORMATION ACROSS THE BORDERS OF THE REPUBLIC OF SOUTH AFRICA (“RSA”)**

23.1 Personal information of data subjects may not be sent to third parties outside of the RSA. If it is necessary to send personal information across the borders of the RSA, the Information Officer must be consulted, who must approve all such transmissions.

23.2 The Information Officer must consider whether any of the following circumstances is present before approval is given:

23.2.1 the third party is subject to a law, binding corporate rules (as prescribed in POPIA) or a binding agreement, which provides an adequate level of protection of that information, and which is like the protection under POPIA;  
or

23.2.2 the data subject has provided written consent; or

23.2.3 it is necessary in terms of a contract between the data subject and the Association; or

23.2.4 it is necessary for a contract concluded between the Association and the third party in the interest of the data subject; or

23.2.5 the transfer is for the benefit of the data subject; it is not reasonably practicable to obtain his/her/its consent and if it was possible the data subject was likely to provide consent.

23.3 ‘Cloud’ storage of records must comply with the requirements of POPIA.

## **24. HISTORICAL, STATISTICAL AND RESEARCH PURPOSES**

Personal information may, in certain circumstances, be used for historical, statistical and research purposes if it is not published in an identifiable form. The Information Officer must be consulted and approve all processing of personal information for historical, statistical and research purposes to ensure that it may occur and that safeguards are in place to protect the privacy of data subjects.

## **25. MARKETING ACTIVITIES**

- 25.1 Direct marketing, including unsolicited electronic marketing, of products and services of the Association may only be directed to members and other persons who have provided written consent for such purposes as prescribed.
- 25.2 Direct marketing must be distinguished from communication with members regarding normal communication, as may be required from time to time.
- 25.3 A data subject may object to the processing of his/her/its personal information for purposes of direct marketing.
- 25.4 A data subject must consent on the prescribed form for the processing of his/her/its personal information for purposes of unsolicited electronic marketing. A data subject may only be requested once for consent.
- 25.5 The Association may process personal information for purposes of unsolicited electronic marketing of bona fide members in the following circumstances:
  - 25.5.1 their contact details were obtained when they became members of the Association;
  - 25.5.2 for the purpose of the direct marketing of the Association's own services (e.g., reminders and invites to participate); and
  - 25.5.3 if they were given a reasonable opportunity to object to the use of their electronic details when the information was collected and every time a marketing communication is provided (i.e., "opt out").
- 25.6 Direct marketing communications must contain the Association's details, including contact details to which the recipient may send a request that such communications cease.
- 25.7 All direct marketing initiatives must also comply with the provisions of the Consumer Protection Act 68 of 2008.

## **26. PROFILING**

- 26.1 Decisions, which are based solely on the automated profiles of persons, for example, related to their performance at work or health, and which may have legal consequences or have a substantial impact on those persons, are not permitted unless it is done in terms of a contract, a law, or a code of conduct subject to the requirements of POPIA.
- 26.2 Profiling of any person or entity may only occur after consultation with and approval by the Managing Director and the Information Officer on the conditions stipulated by them in accordance with the requirements of POPIA.

## **27. INFORMATION REGULATOR**

- 27.1 The Association is accountable to the Information Regulator to ensure that personal information is processed lawfully and without transgressing the privacy of any data subject.
- 27.2 If the law does not authorise the processing of certain personal information and consent cannot be obtained for this purpose, the Information Regulator may be approached for permission or an exemption from POPIA for such processing. If this is required, the Information Officer must approach the Information Regulator.
- 27.3 All decisions of the Information Regulator impacting on the processing of personal information by the Association must be communicated to employees and this Policy and/or other policies must be updated, as may be necessary, to reflect these decisions.

## **28. SECURITY COMPROMISES**

- 28.1 Any compromise of the security of personal information in the possession or under the control of the Association, which includes unauthorised and unlawful access to such information, poses serious risks to the Association. Significant fines may, for example, be imposed by the Information Regulator and/or liability may be incurred for damages as provided for in the law.
- 28.2 If there are reasonable grounds to believe that the personal information of a person has been accessed or acquired by an unauthorised person, it must be reported without delay to the Information Officer, who in turn must advise the Managing Director. Where the Information Officer is involved or allegedly involved in a security compromise, such compromise or alleged compromise must be report to the Managing Director / any director / partner / the auditor / accountant of the Association.
- 28.3 All security or alleged security compromises will result in an investigation of the incident.

- 28.4 An employee, who is responsible for a security compromise, intentionally or unintentionally, in respect of personal information as well as a person who fails to report a security compromise or potential security compromise of which he/she is aware must receive appropriate remedial advice and training and may be subject to appropriate action as may be appropriate such as disciplinary action in the case of employees.
- 28.5 Access to personal information by employees who deliberately or repeatedly violate security mechanisms or compromise the privacy of a data subject's personal information must be suspended until the appropriate remedial action has been determined.
- 28.6 The Information Officer is responsible to report security compromises to the Information Regulator and the persons whose privacy has been compromised as provided for in POPIA.

## **29. COMPLAINTS**

- 29.1 Any complaint, concern, or question regarding the processing of personal information by the Association must be submitted in writing to the Information Officer. If the Information Officer is involved or allegedly involved in the matter, the complaint, concern, or question must be submitted in writing to the Managing Director / any director / partner / auditor / accountant of the Association.
- 29.2 Employees, who are concerned or dissatisfied with the processing of their personal information by the Association, may institute the complaints process as provided for in the Association's workplace policies.
- 29.3 Any person, who is concerned or dissatisfied with the processing of his/her/its personal information by the Association, may lodge a complaint with the Information Regulator, when possible, and he/she/it may not be prohibited from doing so.
- 29.4 The Information Officer must make serious efforts to resolve queries and complaints pertaining to the processing of personal information.

## **30. VERIFICATION OF COMPLIANCE WITH POLICY AND AUDIT**

- 30.1 The Association reserves the right to audit all processing activities of personal information in its possession or under its control from time to time to ensure compliance with this Policy and the law.
- 30.2 The Information Officer may verify compliance with this Policy and the law through various methods, including but not limited to periodic walk-throughs, business tool reports, compliance audits (internal and external) and any form of electronic monitoring.

**31. NON-COMPLIANCE WITH THIS POLICY**

- 31.1 Any non-compliance or alleged non-compliance with this Policy or any relevant legislation will result in an investigation of the non-compliance or alleged non-compliance.
- 31.2 Any violation of this Policy or any relevant legislation will be dealt with in terms of applicable employee policies or another appropriate mechanism, as may be available and applicable.

**32. IMPLEMENTATION OF THIS POLICY**

- 32.1 The Information Officer must ensure that all employees are provided with a copy of or access to this Policy and are trained in every aspect of this Policy.
- 32.2 All employees must agree in writing to comply with this Policy, such other additional documents arising from this Policy as may be approved from time to time and all relevant legislation before being given access or further access to any personal information.

**33. EFFECTIVE DATE OF POLICY**

This Policy comes into operation on the date of approval by the management team and supersedes all other policies and related documents on the subject matter from the effective date.

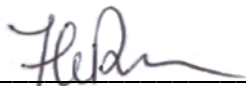
**34. POLICY REVISION**

This Policy must be reviewed and updated at least on an annual basis.



---

Signature of the Executive Director



---

Signature of the Information Officer

Date of Approval: \_\_\_\_\_ 29 June 2021