Protection of Personal Information (POPI) Policy

POPI_GRC_001

Version 1.0 September 2020

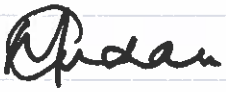
Version Control and Approval	
Document Name	Protection Of Personal Information Policy
Document Number/Version	1.0
Implementation	
Implementation Date	2021/22 Financial Year
Approval	
Date Approved	June 2021
Related Documents	ICT Security Policy (defines data/information protection and privacy) HR Policy (regarding disciplinary procedure of disclosing POPI info) IMC Information Management Policy (in compliance with National Archives Act) Records Retention Policy (as prescribed by National Treasury)
Compiled by: Governance, Compliance & Risk (Nthabeleng Ngoepe, Ebrahim Mayet and Bopila Kadi)	
Reviewed by Statutory Reporting, Risk, Governance and Compliance Manager	
Name	Mompoloki Olerile
Signature	
Reviewed by CFO	
Name	Ikalafeng Diale
Signature	 Date
Recommended by CEO	
Name	Thamsanqa Mdontswa
Signature	Date
Recommended by RMC	
Name	Bhekokwakhe Henry Gutshwa
Signature	 Date
Recommended by ARC	
Name	Michelle Pillay: ARC Chairperson
Position	Chairperson: Audit and Risk Committee
Signature	 Date
Approved by the Board	
Name	Chris Mudau
Position	Chairperson of the Accounting Authority
Signature	 Date

Table of Contents

1. Definitions and Terms

Terms/Acronym	Definition
SASSETA	Safety and Security Sector Education and Training Authority.
Accounting Authority	The Board of SASSETA.
Audit & Risk Committee	A Committee that is charged with, amongst others, the responsibility of overseeing the compliance processes of SASSETA.
Risk Management Committee	A Committee appointed by the Audit and Risk Committee to review the SETA's system of risk management, including compliance risks.
CEO	The Chief Executive Officer of SASSETA.
Information Management Function	The department(s) or team(s) responsible for advising on and managing the POPI Policy within a business or SETA (Information Management Centre - IMC).
Information Management Risk	Failure (or perceived failure) to comply with SASSETA values, applicable laws, regulations and standards that are relevant to the protection of personal information or its ensuing activities, which could damage SASSETA's reputation, lead to legal or regulatory sanctions and/or financial loss.
Information Officer	The official responsible for managing the POPI Policy throughout SASSETA.
Data Subjects	The Accounting Authority, all Governance Structures, CEO and employees and any person/entity/body/individual/company are data subjects whose information is supplied, hosted or given to SASSETA or requested by SASSETA.
POPIA	The Protection of Personal Information Act No. 4 of 2013 (promulgated December 2018).

1.1 Regulatory framework

Related Statutory and Regulatory Frameworks:

a. Protection of Private Information Act 4 of 2013;
b. Promotion of Access to Information Act (PAIA) Act 2 of 2000;
c. Electronic Communications Act 36 of 2005;
d. National Archives and Record Services of South Africa Act 30 of 2007;
e. Promotion of Administrative Justice Act (PAJA) Act 3 of 2000; and
f. Regulation of Interception of Communications Act (RICA) of 2013.

2. Introduction

The Protection of Personal Information Act (POPIA) No. 4 of 2013 (promulgated in December 2018) states the compliance requirements for processing of personal information by South African entities in order to promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.

To ensure compliance to the POPIA, SASSETA developed the Protection of Personal Information (POPI) Policy to outline its compliance approach, as a skills development Sector Education and Training Authority (SETA) in administering and enforcing aspects of the relevant promulgated laws, regulations, directives, prescripts and standards of good practice. The Policy also provides the key elements of SASSETA's compliance approach and the adherence/compliance to the policy, the associated risks and staff and stakeholder awareness relating to the protection of personal information and data.

2.1 Purpose

SASSETA has developed the POPI Policy to formalise its approach to complying and enforcing the law. The Policy and the other SETA's relevant approved policies enables the Board, Management and all employees, representatives and stakeholders to understand the SETA's approach to achieving compliance with regards to the protection of personal information and its custodianship. Further,

SASSETA developed the POPI Policy as a basis for developing compliance with the confidentiality of personal information and the secure custodianship thereof.

The SETA strives to enforce compliance effectively, efficiently and equitably in laws and regulations governing the protection of personal information relating to skills development programmes, skills development levies contributors, learners, bursars, skills and training service providers (universities, technical colleges and TVET's), evaluators, assessors, moderators, verifiers, bidders, staff and other external service providers.

This Policy also sets the standard for suitable protection of personal information as required by The Protection of Personal Information Act No. 4 of 2013 (promulgated December 2018).

2.2 Scope and Applicability

This Policy applies to:

- The Accounting Authority and all governance structures within SASSETA;
- The Chief Executive Officer and all employees of SASSETA;
- SASSETA representatives or any parties acting on behalf of SASSETA; and
- SASSETA external stakeholders and service providers.

2.3 Objectives

The key objectives of the POPI Policy are as follows:

a. To develop, enable and manage a policy that promotes an ethical culture and a commitment to compliance with the protection of personal information and any related policies, laws, regulations, promulgations, directives and relevant prescripts or standards of good practice;

b. To establish, manage and monitor mechanisms and policies, procedures, standards and guidelines that prevent and detect non-compliance with protection of personal information;

c. To implement a policy to identify, prioritise and enable the effective and efficient management of personal information protection risks facing the SETA;

d. To limit exposure to lawsuits, financial losses, sanctions and fines while remaining compliant with protection of personal policies, laws, regulations, promulgations, directives and relevant prescripts or standards of good practice; and

e. To promote good controls and integrity in information and data subject management throughout the SETA.

3. Accountability

Information Officer

In accordance with the POPI Act, the Chief Executive Officer of SASSETA is the appointed Information Officer and is responsible for developing, publishing, implementing and maintaining a POPI Policy, after presentation for recommendation to RMC and ARC and approval by the Board, which addresses all relevant provisions of the Act, including but not limited to:

3.1. The appointment of deputy Information Officers (Executives of respective Departments)

3.2. Ensuring that the appropriate policies and controls are in place for validating the Information Quality and integrity of personal information by reviewing the Act and periodically updating the policy.

3.3. Ensuring that the POPI Policy induction training takes place for all existing and new staff.

3.4. Ensuring that periodic communication and awareness on POPI Act responsibilities takes place.

3.5. Ensuring that Privacy Notices for internal and external purposes are developed, implemented, published and monitored.

3.6. Enforcing compliance of all regulatory requirements of the Act, by SASSETA, with the conditions for the lawful processing of personal information by means of conducting and monitoring POPI assessments with the respective departments of the SETA.

3.7. Managing Data subject information requests made to SASSETA pursuant to the POPI Act.

3.8. Approving special requests for unusual or controversial disclosures of personal data.

3.9. Working with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of this POPI Act in relation to the business.

3.10. Ensuring that appropriate and adequate Security Safeguards in line with the POPI Act for personal information are in place.

Any deviations from this policy or breach thereof or incidents that may relate to such a possibility shall be reported to the SASSETA Information Officer or his delegated representative.

4. Processing Limitation

Control, Collection and Processing of Personal Information

The scope of this aspect of the policy is defined by the provisions within the POPI Act, Condition 2.

4.1. Each department within SASSETA undertakes to comply with the provisions of the Act (sections 9 – 12 inclusive), subject to the forms of consent.

4.2. Personal information may only be processed in a fair and lawful manner and only with the consent of the data subject.

4.3. SASSETA undertakes to collect personal information in a legal and reasonable way and to process the personal information obtained from the data subject for the originally intended purpose for which it was requested.

4.4. SASSETA undertakes to gain written consent where appropriate; alternatively, a recording of the verbal consent shall be kept.

4.5. SASSETA shall compile a POPI Inventory of Documents Control as part of the quality management procedure to identify all instances of personal information in the SETA, which shall illustrate (demonstrate) commitment to protect and use of information in a manner that facilitates transparency and in compliance with the Act.

5. Purpose Specification

5.1. The scope of this aspect of the policy is defined by the provisions of the Act Condition 3, subject to retention periods.

5.2. Personal information may only be processed for specific, explicitly defined and legitimate reasons.

5.3. SASSETA is compelled to keep effective records of personal information and undertakes not to retain information for a period longer than required and in compliance with a Records Retention Policy. Information shall be disposed at the end of the retention period in such a way that it cannot be reconstructed.

5.4. SASSETA shall establish the retention periods for at least the following categories of data:

a. Board and Committee members
b. CEO and Staff
c. Skills Development Levies contributors
d. Learners and Bursars
e. Skills and Training Service Providers

f. Evaluators, Assessors, Moderators and Verifiers

g. Bidders, other External Stakeholders and Service Providers.

6. Further Processing Limitation

The scope of this aspect of the policy is defined by the provisions of the Act, Condition 4.

6.1. SASSETA undertakes to comply with the Act, Condition 2 in terms of processing limitation, section 15.

6.2. Personal information may not be processed for a secondary purpose unless that processing is compatible with the initial purpose.

6.3. Processing of personal information obtained from data subjects shall not be undertaken in an insensitive or wrongful manner which may intrude on the privacy of the data subject.

7. Information Quality

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 5.

7.1. SASSETA shall comply with all the aspects of Condition 5, section 16.

7.2. SASSETA shall ensure that accurate, appropriate and sufficient/enough information is on record of its data subjects and shall regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

7.3. Accuracy

7.3.1. ICT systems should be designed, where possible, to encourage and facilitate the entry of complete, accurate and valid data.

7.3.2. Data on any individual shall be held in as few places as necessary, and all staff shall be discouraged from establishing unnecessary additional data sets.

7.3.3. Effective procedures shall be in place so that all relevant systems are updated when information about any individual (data subject) changes.

7.3.4. Staff who keep more extensive and detailed information about individuals ought to be given additional guidance on accuracy in record keeping.

7.4. Updating

7.4.1. Information Officer or his Deputy Information Officer shall review all personal information on an annual basis.

7.5. Archiving

7.5.1. Archived electronic records of SASSETA shall be stored securely off site.

7.5.2. Paper record archiving takes place using the appointed external service provider.

7.5.3. A certificate of destruction shall be obtained for each batch of archived documents that have been destroyed.

SASSETA further also undertakes not to provide any documentation to a third party or service provider without the consent of the data subject, except where it is necessary for the proper execution of the service as expected by the data subject.

8. Openness

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 6.

8.1. In line with Conditions 6 and 8 of the Act, SASSETA is committed to ensuring that in principle, data subjects whose information is collected shall be aware of the purpose for the data being collected and processed, what types of disclosures are likely; and how to exercise their rights in relation to the data.

8.2. Data Subjects shall generally be informed in the following ways:

8.2.1. Board and Committee Members, CEO and Staff - through this policy.

8.2.2. Skills Development Levy Contributors, Learners, Bursars, Skills and Training Service Providers, Evaluators, Assessors, Moderators, Verifiers, Bidders, Suppliers and other interested parties - through the SASSETA Privacy Notice.

8.3. Whenever data is collected, the number of mandatory fields shall be kept to a minimum and data subjects shall be informed which fields are mandatory and why.

9. Security Safeguards

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 7, section 19 to 22.

9.1 This section of the policy only addresses security issues relating to personal information.

9.2 Personal information shall be kept secure against the risk of loss, unauthorised access, interference, modification, destruction and disclosure.

9.2.1 Specific risks – the following risks have been identified:

9.2.2 Staff with access to personal information could misuse it.

9.2.3 Staff may be tricked into giving away information, either about any category of stakeholders or colleagues, especially over the phone, or through "social interaction".

9.2.4 Hacking of personal records.

9.3 Setting security levels

9.3.1 Access to information on the main SASSETA logical security database shall be controlled by the ICT function in accordance with the ICT Security Policy and the associated User Account Management Policy.

9.3.2 SASSETA shall make use of diagnostic methods and tools where available to identify security levels required for each record held which contains Personal Information.

9.3.3 Non-Disclosure agreements shall be completed with all staff who have access to physical personal records in paper or digitised format.

9.4 Security measures

9.4.1 SASSETA shall ensure that all necessary controls are in place in terms of access to personal information and included in the ICT Security Policy.

10. Data Subject Participation

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Condition 8, sections 23 to 25 inclusive.

10.1. Data subjects may request where their personal information is held, as well as the correction and/or deletion of any personal information held about them, and in both cases be provided with proof of the update or deletion of their information.

10.2. Data subject access requests shall be in writing and shall be administered by the Information Officer. All staff are required to pass on anything which might be a data subject access request to the Information Officer or Deputy Information Officer without delay in all instances.

10.3. Requests for access to personal information shall be handled in compliance with the POPI Act and in compliance with the Promotion of Access to Information Act (PAIA), as well as the Promotion of Administrative Justice Act (PAJA

10.4. Provision for verifying identity

10.1.1 Where the individual making a data subject access request is not personally known to the Information Officer or Deputy Information Officer, their identity shall be verified, and the request shall be reviewed and authorised before handing over any information.

10.5 Charging

10.5.1 Fees for access to personal information shall be handled in compliance with the PAIA Act.

10.6 Procedure for granting access

10.6.1 Procedures for granting access to personal information shall be handled in compliance with the PAIA Act, as defined in the SASSETA PAIA Policy/Manual.

11. Processing of Special Personal Information

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Part B, sections 26 to 33.

11.1. Special personal information includes criminal behaviour relating to alleged offences or proceedings dealing with alleged offences.

11.2. Unless a general authorisation from the Chief Executive Officer has been obtained, alternatively a specific authorisation relating to the different types of special personal information applies, a responsible party is prohibited from processing any special personal information request.

12. Prior Authorisation

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Chapter 6. Prior Authorisation

12.1. SASSETA to develop procedures/guidelines for the compliance and adherence to the process of Prior Authorisation in terms of sections 57 to 59 inclusive.

13. Direct Marketing, Directories and Automated Decision Making

The scope of this aspect of the policy is defined by the provisions of the POPI Act, Chapter 8.

SASSETA undertakes to comply with the POPI Act Chapter 8, sections 69 to 71.

13.1. Opting in

13.1.1. Whenever data is first collected which might be used for any marketing purpose, this purpose shall be made clear, and the Data Subject shall be given a clear opportunity to opt in.

13.2. Sharing lists

13.2.1. SASSETA to consider the development of guidelines for sharing lists (or carrying out joint or reciprocal mailings) where it is warranted and only on an occasional and

controlled basis. Details shall only be used for any of these purposes where the Data Subject has been informed of this possibility, along with an option to opt out, and has not exercised this option.

13.2.2. SASSETA undertakes to obtain external lists only where it can be guaranteed that the list is up to date and those on the list have been given an opportunity to opt out.

13.3. Electronic contact

13.3.1. Whenever e-mail addresses are collected, any future use for marketing shall be identified, and the provision of the address made optional, however, from an operational perspective the emails of relevant staff may have to be provided on the SASSETA website.

14. Staff Training and Acceptance of Responsibilities

14.1. The scope of this aspect of the policy is written in support of the provisions of the POPI Act, Chapter 5, Part B.

14.2. Information for staff is contained in this policy document and other materials made available by the Information Officer or Deputy Information Officer.

14.3. Induction

14.3.1. The Information Officer shall ensure that all staff who have access to any kind of personal information shall have their responsibilities outlined during their induction procedures.

14.4. Continuing training

14.4.1. SASSETA shall provide opportunities for staff to explore POPI Act issues through training, team meetings, awareness and communications and consultations.

Section 69 Direct marketing by means of unsolicited electronic communications

https://popia.co.za/section-69-direct-marketing-by-means-of-unsolicited-electronic-communications/

1. The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic

communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject—

1. has given his, her or its consent to the processing; or
2. is, subject to subsection (3), a customer of the responsible party.

2.

1. A responsible party may approach a data subject—
    1. whose consent is required in terms of subsection (1)(a); and
    2. who has not previously withheld such consent,
    3. only once in order to request the consent of that data subject.
2. The data subject's consent must be requested in the prescribed manner and form.

3. A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of subsection (1)(b)—
    1. if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
    2. for the purpose of direct marketing of the responsible party's own similar products or services; and
    3. if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free

of unnecessary formality, to such use of his, her or its electronic details—

1. at the time when the information was collected; and

2. on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

4. Any communication for the purpose of direct marketing must contain—

    1. details of the identity of the sender or the person on whose behalf the communication has been sent; and

    2. an address or other contact details to which the recipient may send a request that such communications cease.

5. "Automatic calling machine", for purposes of subsection (1), means a machine that is able to do automated calls without human intervention.

15. Breach in Implementing the Policy

A data subject who is of the view that personal information/documentation has been forwarded to a third party without their express approval, may lodge a grievance by following the internal grievance processes and procedures.

16. Policy Accountability

The Chief Executive Officer is accountable for the overall policy implementation of the Policy and reserves the right to intervene and take necessary steps when the policy is not adhered to.

17. Policy Implementation

The Policy shall upon approval, be communicated to all staff members and then implemented.

18. Amendment and adoption

This Policy shall be reviewed by Executive Management for recommendation by the Risk Management Committee and the Audit and Risk Committee and approval by the Board every two years or upon significant amendment(s) to SASSETA's regulatory environment.

Any amendments to this Policy shall only be effective upon approval by the Board of SASSETA.

19. Policy Validity

The policy will be reviewed every two years or as and when the need arises.