| | | | | |
|---|---|---|---|---|
| Shiloh MINISTRIES | Document Number | POL-001 | Author | External Legal |
| | Revision | 01 | Reviewer | P Theron |
| | Document Title | POPI Policy | Approved By | Board |
| | Effective Date | 24/01/2023 | Approval Date | 24/01/2023 |

# SHILOH POPI POLICY

# POL-001

# POPI POLICY

## 1 INTRODUCTION

1.1. Shiloh Ministries NPC (hereafter "the Ministry") is a registered Non-Profit Company with limited liability duly incorporated under the laws of South Africa.

1.2. The Ministry specialises in the Preaching of the Word of God, as described in its Constitution, and this Policy.

1.3. The Ministry is a Responsible Party of Protected Information and Special Protected Information (hereafter "Protected Information") as defined under the Protection of Protected Information Act 4 of 2013 (hereafter "POPIA").

1.4. The Ministry guarantees its commitment to protect the Data Subject's privacy and ensure that their Protected Information is used appropriately, transparently, securely, and in accordance with the applicable laws of the Republic of South Africa.

## 2 OBJECTIVE

This Policy aims to create a compliance framework and provide transparency around collecting, processing, storage, sharing, protecting, and destroying Protected Information.

Additional objectives are:

2.1. To adhere to the legal requirements of the laws of the Republic of South Africa.

2.2. To align policies and processes with the ISO9001:2015 standard.

2.3. To outline the Ministry's policy on the principles, procedure, and management of Protected Information.

2.4. To inform the "Data Subject", defined by Section 1 of POPIA, as to the manner in which their Protected Information is used, protected, disclosed and destroyed.

2.5. To promote best practice principles and standardise the processing of Protected Information by the Ministry.

2.6. To protect the Ministry's reputation and limit the risk of information breach.

2.7. Protect the Data Subject against loss or breach of their Protected Information. and

2.8. Promote safe record-keeping practices.

## 3 DEFINITIONS

3.1. **Approved Supplier** shall mean an individual granted access to the premises to deliver products and services as requested and approved by the Ministry.

3.2. **Business of the Ministry** shall be to preach and teach the Word of God and promote spiritual growth and maturity whilst enabling members to interact and form part of a strong Church and community.

3.3. **Clients** shall include but not be limited to congregational members and visitors, as may be the case.

3.4. **Child** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him-or herself. The Ministry will from time to time have to process Protected Information of a child who may belong to a Data Subject, which use will require the competent person's consent.

3.5. **Ministry** refers to Touch the Nations Ministries with Registration Number NPC 2022/556564/08

3.6. **Common Areas** shall include the reception, designated break areas, cafe, kitchen and outside seating area.

3.7. **Competent person** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

3.8. **Consent** means the voluntary, specific and informed expression of will.

3.9. **De-identify**, in relation to Protected Information of a data subject, means to delete any information that:

3.9.1. Identifies the data subject.

3.9.2. Can be used or manipulated by a reasonably foreseeable method to identify the data subject.

3.9.3. Can be linked by a reasonably foreseeable method to other information that identifies the data subject.

3.10. **Data Subject** means the natural or juristic person to whom the Protected Information relates.

3.11. **Direct Communication** means approaching a Data Subject personally to offer them a Ministry specific product or service.

3.12. **Information Officer** means, in relation to the Ministry, an individual that is part of the executive management of the Ministry as contemplated in Section 1 of the Promotion of Access to Information Act. Details of this individual to be confirmed in clause 28 hereof.

3.13. **POPIA** means the Protection of Protected Information Act, No. 4 of 2013.

3.14. **Protected Information** means information relating to an identifiable, living, natural person, or an identifiable, existing juristic person, as defined in Section 1 of POPIA and includes information relating to:

3.14.1. Race, gender, sex, pregnancy, marital status, mental health, well-being, disability, religion, belief, culture, language and birth.

3.14.2. Education, medical, financial, criminal or employment.

3.14.3. Identity number, electronic and physical addresses, telephone numbers and online identifiers.

3.14.4. Biometric information.

3.14.5. Personal opinions, views or preferences. and

3.14.6. Correspondence sent by a person implicitly or explicitly of a personal nature or confidential.

3.15. **Processing** means any operation or activity, whether or not by automatic means, concerning Protected Information, including:

3.15.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use.

3.15.2. dissemination by means of transmission, distribution or making available in any other form.

3.15.3. merging, linking, as well as restriction, degradation, erasure or destruction of information.

3.16. **Record** means any recorded information, regardless of form or medium, including any of the following:

3.16.1. writing of any material.

3.16.2. information produced, recorded or stored employing any tape-recorder, computer equipment, whether hardware or software or both, or other devices, and any material subsequently derived from information so produced, recorded or stored.

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

3.16.4. book, map, plan, graph or drawing.

3.16.5. photograph, film, negative, tape or other devices 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.

3.16.6. in the possession or under the control of a responsible party.

3.16.7. whether or not a responsible party created it. and

3.16.8. regardless of when it came into existence.

3.17. **Responsible Party** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing Protected Information.

3.18. **Re-identify**, in relation to Protected Information of a data subject, means to resurrect any information that has been de-identified, that—

3.18.1. Identifies the data subject.

3.18.2. Can be used or manipulated by a reasonably foreseeable method to identify the data subject. or

3.18.3. Can be linked by a reasonably foreseeable method to other information that identifies the data subject.

3.19. **Special Protected Information** means information relating to:

3.19.1. The religious, philosophical, or political beliefs of the Data Subject.

3.19.2. The race or ethnic origin of the Data Subject.

3.19.3. The financial status, contributions, income, or expenses of the Data Subject.

3.19.4. Trade union membership of a Data Subject.

3.19.5. Health or sex life of a Data Subject.

3.19.6. The biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs) of a Data Subject.

3.19.7. The criminal behaviour and records of a Data Subject. and

3.19.8. Any information concerning a child.

## 4 POLICY STATEMENT

The Ministry collects and uses Protected Information of employees, individuals, Clients and corporate entities with whom it works in order to operate and carry out the Business of the Ministry effectively.

The Ministry regards the lawful and appropriate Processing of all Personal Information and Special Personal Information (hereinafter collectively referred to as "**Protected Information**") as crucial to successful service delivery and essential to maintaining confidence between the Ministry and its stakeholders. The Ministry, therefore, fully endorses and herewith adheres to the principles of POPIA.

## 5 SCOPE & APPLICATION

5.1. The Policy applies to all employees, directors, volunteers, voting members, agents and sub-contractors, or such appointees of the Ministry.

5.2. This policy also applies to all stakeholders, Clients or any identifiable Data Subjects of the Ministry in terms of POPIA.

5.3. The provisions of the Policy apply to both on and off-site Processing of Protected Information.

5.4. The Policy will be made available upon request to the Information Officer of the Ministry.

5.5. This Policy will be read with and implemented alongside other Ministry Policies, including but not limited to the Privacy, Internet, Email and System Use Policy and the Record Retention Policy.

## 6 RESPONSIBLE PARTIES

6.1 The Information Officer will be responsible for this policy's management, training and administration.

6.2 The policy will be reviewed annually to ensure it reflects and adheres to the latest POPI practice.

6.3 The Information Officer, Deputy Information Officer, and all managers and supervisors are responsible for the implementation thereof.

6.4 Employees must adhere to and apply the policy principles.

## 7 LEGISLATIVE FRAMEWORK

The following Acts, Rules and regulations apply to this policy:

9.1. The Constitution, Charter and religions in South Africa (Chapter 7 Vol 1) [2014]

9.2. Protection of Protected Information Act 4 of 2013 as amended (hereinafter POPIA).

9.3. The Consumer Protection Act 68 of 2008 (hereinafter the CPA).

9.4. The Companies Act, No 71 of 2008

9.5. The Compensation for Occupational Injuries and Diseases Act, No 130 of 1993:

9.6. The Basic Conditions of Employment Act 75 of 1997 (hereinafter the BCEA)

9.7. The Employment Equity Act 55 of 1998 (hereinafter the EEA)

9.8. Labour Relations Act 66 of 1995 (hereinafter the LRA.)

9.9. The Unemployment Insurance Act 63 of 2002 (hereinafter the UIA.)

9.10. Tax Administration Act 28 of 2011 (hereinafter the TAA.)

9.11. The Income Tax Act 58 of 1962 (hereinafter the ITA.)

9.12. The Value Added Tax Act 89 of 1991 (hereinafter the VAT.)

9.13. Skills Development Act, Act 97 of 1998.

9.14. Electronic Communications Act 25 of 2005 (hereinafter the ECA.)

9.15. Promotion of Access to Information Act 2 of 2000

## 8 PROCESSING JUSTIFICATION

The Processing of Protected Information shall be done upon the Data Subject and/or Responsible Party's consent and instruction, for the purpose of:

8.1 Performing such administrative and functions as required to fulfil the Ministry' contractual obligations to Clients.

8.2 Promote the Ministry' legitimate interests, including but not limited to managing, operating or promoting the Ministry.

8.3 Internal and external reporting as may be required.

8.4 In compliance with or to fulfil a legal obligation, whether contractually or otherwise.

8.5 To protect the vital interests of any individual or Client.

8.6 Limiting liability for ourselves, our parent Ministry, subsidiaries, Clients or third parties.

8.7 Administration of agreements.

8.8 Providing products and services to Clients.

8.9 Detecting and prevention of fraud, crime, money laundering and other malpractice.

8.10 In connection with legal proceedings.

8.11 Staff administration and employment legislation compliance.

8.12 Keeping of accounts and records.

8.13 Complying with legal and regulatory requirements.

## 9 INFORMATION REGISTER

The Ministry, for its justified purpose, shall Process the following Information:

| Record Type | Protected Information Processed |
|---|---|
| **General Church (NPC) Records** [Juristic Persons / Entities] | Notice and minutes of all shareholders & director meetings, Resolutions adopted, and documents made available to Directors & Shareholders, Copies of reports presented at the annual general meeting of the Ministry, Copies of annual financial statements required by the Act, Copies of accounting records as required by the Act. |
| **Ministry Management Records** [Juristic Persons / Entities / Natural Person] | Directors / Shareholders: [Name, Surname, Date of Birth, ID Number, Physical and Postal address, Contact details, Ministry Shareholding, Appointment date, Registration Date], Shareholder loans, Ministry Registration Certificate, Memorandum of Incorporation, Shareholder Agreements, Ministry Rules, Director Register, Securities Register, Register of Ministry Secretary, Auditors, Information and Public Officers. |
| **Congregational Member & Visitor Administrative Records** | Personal Information & Special Personal Information as contained on the Membership Application Form which may include: Name, Surname, Telephone, Email, Birthdate, Physical Address, Gender, Marital Status, Acceptance to Statement of Faith, Apostolic Transition Course Completion Status & Result, Natural Family & Dependants. |
| **Employees Onboarding Records** | Appointment Form, Employee Banking Details, Beneficiary Nomination Form. which includes *inter alia* the following information: Marital status, Colour, Race, Age, Gender, Language, Education |

| | |
|---|---|
| [Natural Persons] | information, Financial information, Employment history, ID number, Physical and Postal address, Contact details, Opinions, Occupational Health and Safety and other medical information in the form of medical certificates from registered medical practitioners, Criminal Record, UIF, PAYE, Income Tax, Biometric Data, Union Membership. |
| **Visitor Card** | Name, Surname, Telephone, Email, Age, Birthdate, Address |
| **Disciplinary Record** | Full Employee Record of each Employee specifying the nature of any disciplinary transgressions (Charge), the actions taken by the Employer and the reasons for the actions |
| **Training** | Name, Surname, Email, Telephone Numbers, Address - Location<br>Online Identifier. |
| **Outreach** | Name, Surname, Email, Telephone Numbers, Passport, Next of Kin<br>Medical Information. |
| **Prayer Request** | Dedicated WhatsApp / Call / Email - dedicated intercessors: Name, Surname, Cell Phone, Email, Medical / Financial / Employment / General life matters / Family. Anonymity welcome. |
| **Wedding Register** | Name, Surname (maiden), Telephone, Email, Birthdate, Address<br>ID Book, Birth Certificate. |
| **Funerals** | Name, Surname, Email, Telephone Numbers, Next of Kin<br>Date of Birth & Death. |
| **Covid Register** | Personal Information & Special Personal Information as contained on Membership Application Form which may include: Name, Surname, Telephone, Email, Temperature, Basic Medical Information. |
| **Approved Suppliers** | Name of the legal entity, Names of contact persons, Physical and Postal address, Contact details, Registration number, Ministry Incorporation Documents, Tax & VAT related information, Banking Details, Ultimate beneficial owners. Shareholding information, BBBEE information, Contractual Terms between parties. |

| | |
|---|---|
| **Membership Mailing List** | Personal Information & Special Personal Information: Name, Surname, Telephone, Email, Age, Different Groups Listed on e.g. [General / Prayer / Leaders / Youth/ Management, etc.] |
| **Employee Reference Check** | Credit Check, Criminal, Educational, Empowerment, Disability, Fraud, Anti Competition & Money Laundering Information |

## 10 DATA FLOW AND IMPACT ASSESSMENT

To comply with the standard of the Act, the Ministry, as demonstrated in **POL-001-FORM-01 to 03,** has conducted the necessary GAP, Risk & Impact assessment to identified, investigated and consider:

10.1. What Protected Information it collects and Processes.

10.2. Its accountability role in association with Protected Information.

10.3. Who has primary access and use of the Protected Information.

10.4. The classification of the Protected Information.

10.5. The manner and form in which consent is obtained from the Data Subject.

10.6. The reason for and justification of collection and processing.

10.7. The internal and external data flow and further Processing of Protected Information.

10.8. The quality of the Information source.

10.9. The manner and form in which the Data Subject has been made aware of his/her/its rights and responsibilities towards his/her/its Protected Information.

10.10. Cross-border transfer and processing of Protected Information.

10.11. The security safeguards and measures put in place to protect the Protected Information.

10.12. Statutory and Ministry retention periods according to classification.

10.13. Risk probability, impact, and mitigation actions in case of abuse or breach.

10.14. Responsible and designated individual to act in case of breach or abuse.

## 11 EIGHT PROCESSING CONDITIONS

POPIA is implemented by abiding by eight processing conditions. The Ministry shall abide by these principles in all its processing activities.

### 11.1. Accountability

The Ministry shall ensure that all processing conditions, as set out in POPIA, are complied with when determining the purpose and means of Processing Protected Information and during the processing itself. The Ministry shall remain liable for compliance with these conditions, even if it has outsourced its processing activities.

### 11.2 Processing Limitation

Lawful grounds

11.2.1 The Processing of Protected Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive. The Ministry shall only process Personal Information if one of the following grounds of lawful processing exists:

- 11.2.1.1 The Data Subject consents to the processing.
- 11.2.1.2 Processing is necessary for the conclusion or performance of a contract with the Data Subject or Responsible Party.
- 11.2.1.3 Processing complies with a legal responsibility imposed on the Ministry.
- 11.2.1.4 Processing protects a legitimate interest of the Data Subject.
- 11.2.1.5 Processing is necessary for the pursuance of a legitimate interest of the Ministry or a third party to whom the information is supplied.

11.2.2 The Ministry may only process Special Personal Information under the following circumstances:

- 11.2.2.1 The Data Subject has consented to such processing.
- 11.2.2.2 The Special Protected Information was deliberately made public by the Data Subject.
- 11.2.2.3 Processing is necessary for the establishment of a right or defence in law.
- 11.2.2.4 Processing is for historical, statistical, or research reasons.
- 11.2.2.5 Processing of race or ethnic origin is in order to comply with labour relations and affirmative action laws.

11.2.3 All Data Subjects have the right to refuse or withdraw their consent to the Processing of their Protected Information, and a Data Subject may object, at any time, to the Processing of their Protected Information on any of the above grounds, unless legislation provides for such processing. If the Data Subject withdraws consent or objects to the processing, then the Ministry shall forthwith refrain from processing the Protected Information.

Collection directly from the Data Subject

11.2.4 Protected Information must be collected directly from the Data Subject, unless:

11.2.4.1 Protected Information is contained in a public record.

11.2.4.2 Protected Information has been deliberately made public by the Data Subject.

11.2.4.3 Protected Information is collected from another source, e.g. medical practitioner, with the Data Subject's consent.

11.2.4.4 Collection of Protected Information from another source would not prejudice the Data Subject.

11.2.4.5 Collection of Protected Information from another source is necessary to maintain, comply with or exercise any law or legal right.

11.2.4.6 Collection from the Data Subject would prejudice the lawful purpose of the collection.

11.2.4.7 Collection from the Data Subject is not reasonably practicable.

Purpose Specification

11.2.5 The Ministry shall only process Protected Information for specific purposes as set out in paragraph 8 and 11.2 of the Policy.

**11.3 Further Processing**

New processing activities must be compatible with the original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

11.3.1 Data Subject has consented to further processing.

11.3.2 Protected Information is contained in a public record.

11.3.3 Protected Information has been deliberately made public by the Data Subject.

11.3.4 Further processing is necessary to maintain, comply with or exercise any law or legal right.

11.3.5 Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party.

**11.4 Original Information**

11.4.1 The Ministry shall take reasonable steps to ensure that Protected Information is complete, accurate, not misleading.

11.4.2 The Ministry shall periodically review Data Subject records to ensure that the Protected Information is still valid and correct.

11.4.3 Employees should as far as reasonably practicably follow the following guidelines when collecting Protected Information:

11.4.3.1 Protected Information should be dated when received.

11.4.3.2 A record should be kept of where the Protected Information was obtained.

11.4.3.3 Changes to information records should be dated.

11.4.3.4 Irrelevant or unneeded Protected Information should be deleted or destroyed.

11.4.3.5 Protected Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

**11.5 Openness**

The Ministry shall take reasonable steps to ensure that the Data Subject is made aware of:

11.5.1. What Protected Information is collected.

11.5.2. The purpose of collection and processing.

11.5.3. Where the supply of Protected Information is voluntary or mandatory, and the consequences of a failure to provide such information.

11.5.4. Whether the collection is in terms of any law requiring such collection.

11.5.5. Whether the Protected Information shall be shared with any third party. and

11.5.6. If such Protected Information is to be shared with a third party, obtain the Data Subject's consent to share such Protected Information, save for instances where the Ministry is legally obliged to share the Protected Information.

11.6. **Data Subject Participation**

11.6.1. The Data Subject has the right to request access, amendment, or to delete their Protected Information. All such requests must be submitted in writing to the Information Officer in the prescribed form, Annexure B (Government Gazette Form 2), which process, rights and limitations shall be more fully covered in paragraph 18 hereof.

11.6.2. The Ministry shall not disclose any Protected Information to any party unless the requester's identity has been verified.

11.7. **Confidentiality**

11.7.1. Employees, Agents and Business Partners herewith undertake to treat all Protected Information as Confidential and shall only share this with individuals within the Ministry structure on a need-to-know basis relevant to their designation, role and duties within the Ministry.

11.7.2. The Ministry undertakes to secure the confidentiality of Special Personal Information or Child Personal Information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent loss of damage to or unlawful access to such information.

11.7.3. In terms of the Protection of Protected Information Act, all employers and all employees are legally obliged to treat all medical or health information as private and confidential.

11.8. **Security and Storage Safeguards**

11.8.1. The Ministry shall ensure the integrity and confidentiality of all Protected Information in its possession by taking reasonable steps to:

11.8.1.1. Identify all reasonably foreseeable risks to information security (POL-001-FORM-01). and

11.8.1.2. Establish and maintain appropriate safeguards against such risks.

11.8.2. Clean Desk Policy

To prevent unauthorised access to information and promote the security and confidentiality of Protected Information as well as information about our employees, our intellectual property and trade secrets, our Members, and vendors, the Ministry and all of its Employees shall adhere to and maintain a clean desk policy.

11.8.2.1. Employees shall ensure that:

11.8.2.1.1. All sensitive and confidential information, whether it be on paper, a storage device, a whiteboard, or a PC, is properly locked away, cleared, or disposed of, when a workstation, meeting room, or common area, is not in use and/or left unattended for a period exceeding 30 minutes.

11.8.2.1.2. All Protected Information in hardcopy or electronic form, including paper notebooks and printed sheets, and mass storage devices such as CDs, DVDs, and USB drives, be removed from their desks or other places

(printers, fax machines, photocopiers, etc.) when not in use and/or left unattended for a period exceeding 30 minutes.

11.8.3. Clear Screen Policy

11.8.3.1. PC's, tablets and phones containing Protected Information of the Ministry or its Clients must be protected from unauthorised access and may not be left unattended or unlocked.

11.8.3.2. Employees shall ensure that:

11.8.3.2.1. All sensitive information be removed from the screen, and all devices are logged out of programmes containing Protected Information.

11.8.3.2.2. Passwords should never be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

11.8.4. Equipment Safeguarding

PC's, tablets and phones containing Protected Information of the Ministry or its Clients must be protected from unauthorised access and may not be left unlocked when unattended.

11.8.4.1. Employees shall ensure that:

11.8.4.1.1. Computers, laptops and hand-held devices are screen locked when a workspace or device is unoccupied.

11.8.4.1.2. File cabinets containing Confidential or Protected Information must be kept closed and locked when not in use or unattended.

11.8.4.1.3. Keys for accessing drawers or filing cabinets may not be left on a desk.

11.8.4.2. Only authorised personnel may Process Protected Information on their personal computers, laptops or hand-held devices. Which devices shall:

11.8.4.2.1. Be secured in a safe and locked environment if not in use.

11.8.4.2.2. Not be left unattended.

11.8.4.2.3. Where practical, password protection shall be activated for applications that contain or provide access to Protected Information.

11.8.4.2.4. Be secured with commercially acceptable firewalls and security protection software.

11.8.4.2.5. Implement two-factor authentication for passwords.

11.8.4.2.6. Install remote access and deletion software as directed by IT.

11.8.4.2.7. Be secured with a password, fingerprint or retina scan, which password (if used) shall be of reasonable complexity and changed every three months.

11.8.5. Authorised Personnel Only

To prevent unauthorised access to information and promote Protected Information security and confidentiality, the Ministry adheres to a strict, authorised and employee-only access rule. To give effect to this rule, the Ministry shall impose the following restrictions:

11.8.5.1. Employees may not allow personal visitors to access areas not designated as Common Areas.

11.8.5.2. All visitors must report to reception to sign in and receive authorisation to access the premises.

11.8.5.3. Employees may receive authorised personal visitors during designated break times. It is advisable to only permit visitors in Common Areas for a short time and for specific reasons.

11.8.5.4. Employees are responsible for accompanying their visitors at all times.

11.8.5.5. Employees shall only be permitted to access a workstation that has not been assigned to them if the designated Employee is present.

11.8.6. Written records

11.8.6.1. Protected Information records will be kept in safe storage with limited access.

11.8.6.2. When in use, Protected Information records shall not be left unattended in areas where non-staff members may access them.

11.8.6.3. The Ministry shall implement and maintain a "Clean Desk Policy" where all employees shall be required to clear their desks of all Protected Information when leaving their desks for any length of time and at the end of the day, alternatively they shall lock their office to restrict unauthorised access.

11.8.6.4. Protected Information, which is no longer required, should be disposed of as in terms of the Information Retention & Destruction protocols of the Ministry, ensuring the de-identification of persons and their related Protected Information.

11.8.6.5. Any loss or theft of, or unauthorised access to, Protected Information must be immediately reported to the Information Officer to take such legally required steps as may be necessary.

11.8.6.6. The Ministry shall preserve and protect the physical integrity of records by ensuring adequate storage that is secure, dry and insect and rodent-free.

11.8.7. Electronic Records

11.8.7.1. All electronically held Protected Information must be saved according to the Ministry's Policy.

11.8.7.2. All computers, laptops and hand-held devices should be access protected with a password, fingerprint, or retina scan, which password shall be of reasonable complexity, with two-factor authentication.

11.8.7.3. The Ministry shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day.

11.8.7.4. Electronic Protected Information, which is no longer required, must be permanently deleted from the individual device and the relevant database as directed by the Retention & Destruction protocols.

11.8.7.5. Any loss or theft of computers, laptops or other devices which may contain Protected Information must be immediately reported to the Information Officer to take such legally required steps as may be necessary.

11.8.7.6. Electronic records must be regularly backed up in terms of the Ministry 's Policy, with back-ups kept at a secure off-site location.

## 12 DISCLOSURE OF MEDICAL, TRADE UNION AND OTHER SENSITIVE INFORMATION

The Ministry shall only process and disclose such Protected Information to the relevant bodies in compliance to legal or regulatory compliance, industry or federation rules (to which the Ministry or its employees are a member or signatory), if it could be confirmed that the Data Subject:

12.1. Has consented in writing to the disclosure thereof.

12.2. Is aware of the purpose of the processing and disclosure.

12.3. Is aware of whom the Protected Information is disclosed to.

12.4. Has been informed if the disclosure is voluntary or mandatory.

12.5. Has been informed that, should the Data Subject fail to provide the Responsible Person or their mandated Processors with its written consent to disclose the required information, the Ministry or respective body may at its discretion reject the Employee's membership or employment.

## 13 TRANSFER & SHARING OF INFORMATION

13.1. The Ministry may supply the Protected Information to any party to whom the Ministry or its instructing Responsible Party may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

13.1.1. Capturing and organising of data.

13.1.2. Storing of data.

13.1.3. Member communication.

13.1.4. Conducting due diligence checks.

13.1.5. Industrial relational services.

13.1.6. Legal services

13.1.7. Auditing & Accounting Services

13.1.8. Quality Certification Services

13.2. Furthermore, the Ministry may supply Protected Information to anybody enacted in terms of the laws of the Republic of South Africa and in terms of which laws the Ministry is obligated to share such information, which may include but is not limited to:

13.2.1. The South African Revenue Service

13.2.2. The Department of Employment and Labour

13.2.3. The Unemployment Insurance Fund

13.2.4. Industry Bodies as directed by the Department of Trade and Industry.

13.2.5. All bodies and entities as directed by law.

## 14 CROSS-BORDERDER FLOW

14.1. Protected Information may be transmitted or stored in data servers hosted by authorised service providers outside of South Africa. The Ministry will endeavour to ensure that authorised service providers make all reasonable efforts to secure said data and Protected Information.

## 15 RECORD RETENTION & DESTRUCTION

15.1 The Ministry shall adhere to the retention best practice principles, and such other statutory and regulatory requirements as may be applicable. However, the Ministry may retain documents for such extended periods as directed in this Policy to limit its liability or that of its Members.

15.2 Statutory and Ministry Retention & Destruction Periods (*where applicable*)

| Department | Legislation | Record Type | Minimum Statutory Retention Period | Maximum Ministry Retention Policy |
|---|---|---|---|---|
| **Management** | **Companies Act** | Any documents, accounts, books, writing, records or other information that a NPC is required to keep in terms of the Act. | 7 years | 10 years |
| | | Ownership Documents: Registration certificate. Memorandum of incorporation and alterations and amendments. Rules. Securities register and uncertified securities register. Register of Company Secretary and Auditors. | Indefinitely | Indefinitely |
| | | Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) - Register of disclosures of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued | Indefinitely | Indefinitely |

| | | | | |
|---|---|---|---|---|
| | | Notice and minutes of all shareholders meetings, including:<br>▪ Resolutions adopted.<br>▪ Documents made available to holders of securities, Copies of reports presented at the annual general meeting of the Church, Copies of annual financial statements required by the Act.<br>▪ Copies of accounting records as required by the Act<br>▪ Record of directors and past directors, after the director has retired from the Church.<br>▪ Written communication to holders of securities, Minutes and resolutions of directors' meetings, audit committees and directors' committees. | 7 years | 10 years |
| **Promotional Communication** | **Consumer Protection Act** | ▪ Full Client details<br>▪ Contact details of designated individuals and/or of the Ministry itself<br>▪ Quotes: Service rendered, and such amounts, sums, values, charges or fees as agreed between the Parties. | 3 years | 5 years after termination or completion of the ministry relationship and/or contract |
| **Finance** | **Companies Act** | ▪ Copies of annual financial statements required by the Act<br>▪ Copies of accounting records as required by the Act | 7 years | 10 years |
| | **Tax Administration Act & Other** | ▪ Invoices<br>▪ Proof of Payments<br>▪ Accounting Records & notes<br>▪ Management Accounts | 5 years from the date of submission | 10 years |

| | | | | |
|---|---|---|---|---|
| | | ▪ Cash Office Journals/Payments<br>▪ Recons | | |
| | **Income Tax Act** | Amount of remuneration paid or due by him to the Employee.<br>▪ The amount of employees' tax deducted or withheld from the remuneration paid or due.<br>▪ The income tax reference number of that Employee.<br>▪ Any further prescribed information.<br>▪ Employer Reconciliation return. | 5 years from the date of submission | 10 years |
| | **Value Added Tax Act** | ▪ Where a vendor's basis of accounting is changed, the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period.<br>▪ Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS.<br>▪ Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques.<br>▪ Documentary proof substantiating the zero-rating of supplies.<br>▪ Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as | 5 years from the date of submission | 10 years |

| | | | | |
|---|---|---|---|---|
| | | described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address, and VAT registration number of the principal to be ascertained. | | |
| | **Financial Intelligence Centre Act** | All FICA and other related documents as required by the Act. Including Credit Reports, IDs of Directors. Eventual beneficial owners, CIPC Documents, proof of address and such information as normally included in a Client and/or Credit application. | 5 years | 5 years after termination or completion of the contract or purpose. |
| | **Unemployment Insurance Act** | ▪ Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the Employee is employed | 5 years from the date of submission | 5 years after termination or completion of the contract |
| **Human Resources** | **Basic Conditions of Employment Act** | ▪ Employee CV & Educational Information<br>▪ Contact details of Employee<br>▪ Job description<br>▪ Letter of appointment<br>▪ Employment Agreement<br>▪ Attendance (Clock Cards) & leave record. | 3 years | 5 years after termination or completion of the contract |
| | **Employment Equity Act** | Records in respect of the Ministry 's workforce, employment equity plan and other records relevant to compliance with the Act.<br>Section 21 report which is sent to the Director-General | 3 years after the expiry of the plan | 5 years after termination or completion of the contract |

| | | | | |
|---|---|---|---|---|
| | **Labour Relations Act** | Records to be retained by the Employer are the Collective Agreements and Arbitration Awards. | 3 years | 5 years after termination or completion of the contract |
| | | An employer must retain prescribed details of any strike, lock-out or protest action involving its employees. Records of disciplinary transgressions, the actions taken by the Employer and the reasons for the actions | Indefinitely | Indefinitely |
| | **Skills Development Act 97 of 1998*** | All skills development plans or levy payments or submissions | 5 years from the date of entry or submission | 5 years from the date of entry or submission |
| | **Maintenance** | General & preventative maintenance records | | 3 years |
| | **Compensation for Occupational Injuries and Diseases Act*** | Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees. | 4 years | 5 years after termination or completion of the contract |
| | | Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation. | 3 years | 5 years after receipt of the recommendation |
| | | Records of incidents reported at work | Kept for 20 years after treatment has ended | Indefinitely or until Data Subjects passing. |

## 16 RECORD MANAGEMENT

16.1 An efficient records management system should include arrangements for archiving or destroying dormant records to de-identify and preserve documents while also making space for new records, particularly in the case of paper records.

16.2 Records held electronically are covered by the Electronic Communications and Transactions Act and shall be permanently deleted once they reach the Ministry's retention horizon.

16.3 The destruction process shall be managed and approved by the relevant Information Officer.

16.4 Documents may be destroyed after the retention period specified in paragraph 15 of this policy, for the relevant document type has been reached.

16.5 The Ministry Information Officer will annually request each Head of Department/Manager to attend to the destruction of their documents, which requests shall be attended to timeously.

16.6 Heads of Departments/Managers shall ensure that:

16.6.1 All records are examined to ensure that they are suitable for disposal

16.6.2 Files are checked for originals

16.6.3 Original documents must be returned to the holder or data subject thereof, failing which the Ministry should retain them pending such return.

16.6.4 All documents marked for destruction are logged on the destruction registers **POL-001-FORM-003.**

16.6.5 All destruction registers **POL-001-FORM-003** shall be submitted for final review and approval by the Information Officer.

16.7 Any documents flagged by the Information Officer shall be retained, providing a reason for the retention.

16.8 The Information Officer shall retain a copy of all destruction registers.

16.9 Documents and/or records approved for destruction shall be destroyed and de-identified as follows:

16.9.1 Paper records should be shredded or incinerated.

16.9.2 CDs, DVDs, hard disks and other forms of electronic storage should be overwritten with random data, permanently deleted or physically destroyed.

16.9.3 All computers, laptops and hand-held devices should be formatted or be reset to factory settings.

16.10 Approved Service providers, under contract of confidentiality, may dispose of such Protected Information on behalf of the Ministry providing certification that the files have been destroyed in accordance with POPIA.

## 17 DIRECT COMMUNICATION

17.1 All Direct Communications shall contain the Ministry's details and an address or method for the Client to opt out of receiving further promotional communication.

Existing Members

17.2 Direct Communication by electronic means to existing Members is only permitted:

17.2.1 If the customer consented to receive ministry-related information.

17.2.2 If the customer's details were obtained in the context of a service rendered. and

17.2.3 For the purpose of communicating the same or similar services.

17.2.4 The customer must be given the opportunity to opt-out of receiving direct communication on each occasion of direct communication.

Consent

17.3 The Ministry may send electronic Direct Communication to Data Subjects who have consented to receive it. The Ministry may approach a Data Subject for consent only once.

17.4 The Ministry shall keep a record of:

17.4.1 Date of consent.

17.4.2 The wording of the consent.

17.4.3 Who obtained the consent.

17.4.4 Proof of opportunity to opt-out on each Communications contact. and

17.4.5 Record of opt-outs.

## 18 RIGHT TO ACCESS & AMEND PROTECTED INFORMATION

18.1 All individuals and entities may request access, amendment, or deletion of their own Protected Information held by the Ministry, subject to relevant legislation.

18.2 On the prescribed form, requests should be directed to the Information Officer or his/her Deputy Information Officer (The prescribed Form 2, as per Government Gazette 42110 of 14 December 2018, attached hereto as Annexure E).

Who may request Access, Alter or Deletion

18.3 The Information Officer shall verify that the identity of the individual requesting the information is the Data Subject or so authorised, by:

18.3.1 Verifying the ID document of the individual requesting access.

18.3.2 Authenticating a signed power of attorney of the individual providing access to the requester.

18.3.3 Verifying the company resolution providing the requester with authority to do so o.b.o. the company requesting access to their information.

18.4 Parents may request access, alteration, or deletion of a Child's records if it is in the Child's best interest.

18.5 If the Data Subject is an adult and the request for access, alteration, or deletion of records are made by an individual other than the Data Subject, the commissioned written consent of the Data Subject must accompany the request.

18.6 Relatives have no automatic right of access to an adult Data Subject's records. If the Data Subject lacks the mental capacity to consent to the disclosure, the nomination must be made by a person appointed by the court to manage the Data Subject's affairs.

18.7 Any 3rd party if the request is made in compliance with a court order.

18.8 A written directive has been issued by a judge or a magistrate.

Access, alteration or deletion

18.9 Upon receiving a duly completed Form 2 and having satisfied him/herself that the individual is the Data Subject and/or authorised individual, the Information Officer may amend or delete such Protected Information of the Data Subject that is under its control if such information is:

18.9.1 Inaccurate

18.9.2 Irrelevant

18.9.3 Excessive

18.9.4 Out of date

18.9.5 Incomplete

18.9.6 Misleading. or

18.9.7 Obtained unlawfully.

18.10 On receipt of such a request, the Information Officer shall, as soon as reasonably practicable:

18.10.1 Refuse the request

18.10.2 Correct the information

18.10.3 Destroy or delete the information

18.10.4 Provide the data subject with credible evidence that the request has been performed.

Grounds for Refusal

18.11 The Ministry may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which the Ministry may refuse access include:

18.11.1 Protecting Protected Information that the Ministry holds about a third person (who is a natural person), including a deceased person, from unreasonable disclosure.

18.11.2 Protecting commercial information that the Ministry holds about a third party or the Ministry (for example, trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the Ministry, Data Subject or the third party).

18.11.3 If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement.

18.11.4 If disclosure of the record would endanger the life or physical safety of an individual.

18.11.5 If disclosure of the record would prejudice or impair the security of property or means of transport.

18.11.6 If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme.

18.11.7 If disclosure of the record would prejudice or impair the protection of the safety of the public.

18.11.8 The record is privileged from production in legal proceedings unless the legal privilege has been waived.

18.11.9 Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of the Ministry.

18.11.10 Disclosure of the record would put the Ministry at a disadvantage in contractual or other negotiations or prejudice it in commercial competition.

18.11.11 The record is a computer programme. and

18.11.12 The record contains information about research being carried out or about to be carried out on behalf of a third party or the Ministry.

## 19 REMEDIES IF REQUEST FOR ACCESS TO PROTECTED INFORMATION IS REFUSED

Internal Remedies

19.1 The Ministry does not have internal appeal procedures. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the Information Officer.

External Remedies

19.2 If a requestor is dissatisfied with the Information Officer's refusal to disclose information, he/she may complain to the Information Regulator in terms of Chapter 10 of POPIA.

Records that cannot be found or do not exist

19.3 If the Ministry has searched for a record and it is believed that the record does not exist or cannot be found, the requestor will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

## 20 SECURITY PROTOCOLS

20.1 With reference to information processing, the Ministry shall employ and only contract with 3rd Party Service providers that implement industry-grade technology and security principles.

20.2 The Ministry shall endeavour to do all that is reasonably possible to ensure the confidentiality, integrity and availability of the Protected Information under its care.

20.3 Measures shall include the implementation of:

20.3.1 Computer Firewalls

20.3.2 Virus protection software and update protocols

20.3.3 Logical and physical access control

20.3.4 Secure setup of hardware and software making up the IT infrastructure

20.3.5 Off-site storage of all electronic back-ups

20.3.6 Important paper documents will be kept in a fire-proof safe

20.3.7 Compliance with such Health and Safety protocols, as required by law.

## 21 THIRD-PARTY SECURITY RISK REVIEW

| 3rd Party System | Information Collected | Confidentiality | 3rd Party Links | Security | Server Location | Retention Periods | POPI / GDRP Compliant |
|---|---|---|---|---|---|---|---|
| **Microsoft Office 365 OneDrive, Excel, Word, PowerPoint, SharePoint, Bookings, One Note, Outlook, Teams*** | Personal & Special Personal Information | Presumed | No protection or Guarantee | Good. Industry-standard security practices: Identity, devices, apps, emails and documents. Offering Advanced Encryption, Transport Layer Security, Data Loss Prevention Policies, Advanced Threat Protection. | Globally distributed Data Center infrastructures according to GDRP (EU) Standards) | 30-day backup & retention policy executed every 12 hours. User dictates retention of documents. | Compliant |
| **Acrobat Reader*** | Personal & Special Personal Information | None | None | Good. Industry-standard security practices, ISO 27001 compliant | None - Application-Based | None. User dictates retention of documents on local server or device. | Compliant |
| **Preview (Mac)*** | Personal Information | None | None | Good. Industry-standard security practices, ISO 27001 compliant | None - Application-Based | None. User dictates retention of documents on local server or device. | Compliant |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **QuickBooks Online*** | Personal & Special Personal Information | Explicitly excluded | No protection or Guarantee | Good. Data centres. Password-protected login, multi-factor authentication, firewall-protected servers and encryption technology for data at rest and in transit. TRUSTe certified. | Cross-border transfer of Information. Intuit-operated and Amazon Web Services (AWS) servers. | Data will be available in read-only access for 1 year from the date of cancellation or deletion. | Compliant |
| **SAGE VIP Payroll*** | Personal & Special Personal Information | Agreed | No protection or Guarantee | Reasonable security: One layer password protection, Firewall and Intrusion detection, Industry-standard monitoring technologies. SLL security | Unknown. Managed hosted environment at a secure physical location with 24/7 armed security. Data is stored in two alternative locations, accommodating multiple points of failure. | Back-ups performed daily. Data retained for 2 weeks after deletion. | Compliant |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **WhatsApp*** | Personal & Special Personal Information | Agreed | No protection or Guarantee | Triple Layer end-to-end encryption. | Cross-border transfer of Information. Uses 700+ Servers and data centres mainly located in California & Washington. | Minimum legal requirements or such longer periods as may be required for operational purposes. | Compliant |
| **PDF Creator*** | Personal & Special Personal Information | None | None | Good. Industry-standard security practices, 128-bit encryption. | None - Application-Based | None. User dictates retention of documents on local server or device. | Compliant |
| **Adobe Suite** | Personal & Special Personal Information | Agreed | None | Good. Industry-standard security practices, 128-bit encryption of scans unto Adobe Document Cloud | Cross-border transfer of Information. Multi-jurisdiction server and data centres with core situated in Adobe facility in Oregon (US) | Documents are retained as long as the account is active. Transactional user data is retained until customer request deletion. | Compliant |
| **SARS eFiling** | Personal Information | Presumed | No protection or Guarantee | Weak due to Flash player use and migration. | Unknown | Minimum legal requirements or such longer periods as may be consented to. | Pending |

Where applicable*

## 22 IMPLEMENTATION GUIDELINES

22.1 This Policy has been approved and effected by senior management on the effective date as indicated in clause 27 of this document.

22.2 The Ministry has trained all employees on the content and impact of this Policy and POPIA on the Ministry's operational requirements.

22.3 Ongoing awareness campaigns and departmental training will be done where the need arises.

22.4 All new employees and volunteers will be made aware of their responsibilities under the terms of this Policy and POPIA, at induction or through training programs.

22.5 Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all employees and volunteers of the ministry.

22.6 Employee Contracts

22.6.1 An Addendum or insertion containing the relevant consent clauses for using and storing employee information and acknowledging policy will be added to each new and existing Employee's Employment contract.

22.6.2 Employees will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Protected Information, however, it is processed.

22.6.3 Failure to comply will result in the instigation of a disciplinary procedure.

22.7 Volunteers

22.7.1 Volunteers will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Protected Information, however, it is processed.

22.7.2 Failure to comply will result in disciplinary steps and possible ejection.

## 23 VIOLATIONS AND DISCIPLINARY MEASURES

23.1 The Information Officer shall set up such reasonable control measures to preserve and secure documents.

23.2 Violation or abuse of this Policy shall be deemed an offence which shall justify a written or final written warning and termination of employment, office or such position volunteered for as may be applicable.

23.3 Any Person (Definition as per POPIA) who commits any of the following transgressions shall be liable, upon conviction, to a fine or imprisonment or both as directed by POPIA:

23.3.1 Fails to perform a duty imposed on them in terms POPIA.

23.3.2 Falsifies any record by adding to or deleting, or changing any information contained in that record.

23.3.3 Creates, changes or destroys a record without authority to do so.

23.3.4 Fails to create or change a record when properly required to do so.

23.3.5 Provides false information with the intent that it be included in a record.

23.3.6 Without authority, copies any part of a record.

23.3.7 Gains unauthorised access to a record or record-keeping system, including intercepting information being transmitted from one person, or one part of a record-keeping system, to another.

23.3.8 Without authority, connects any part of a computer or other electronic system on which records are kept to any other computer or another electronic system. or any terminal or other installation connected to or forming part of any other computer or another electronic system.

23.3.9 Who without authority modifies or impairs the operation of:

23.3.9.1 any part of the operating system of a computer or other electronic system on which a user's records are kept.

23.3.9.2 any part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept.

## 24 MONITORING, EVALUATION AND REVIEW

This policy and underlying strategies will be reviewed at least annually or as necessary to ensure its continued application and relevance.

## 25 RELATED POLICIES

Effective implementation of this policy requires that it be read together with other Departmental Policies and Forms:

| Document Number | Document Name |
|---|---|
| POL-001-FORM-01 | Impact & Risk Assessment |
| POL-001-FORM-02 | 3rd Party Risk Assessment |
| POL-001-FORM-03 | Destruction Register |
| POL-001-FORM-04 | Policy Acknowledgment & Employee Declaration |
| POL-001-FORM-05 | Government Gazette Form 2 |

## 26 RELATED PROCEDURES

Effective implementation of this policy requires that it be read together with other Departmental Processes & Data Flows:

| Document Number | Document Name |
|---|---|
| POL-001-PRO-01 | Congregational Member Onboarding |
| POL-001-PRO-02* | Mailing & Communication |
| POL-001-PRO-03* | Visitors |
| POL-001-PRO-04 | Covid |
| POL-001-PRO-05* | Prayer Request |

| | |
|---|---|
| POL-001-PRO-06* | Wedding Registry |
| POL-001-PRO-07* | Funerals |
| POL-001-PRO-08A* | Training |
| POL-001-PRO-08B* | Bible School |
| POL-001-PRO-09* | Outreach |
| POL-001-PRO-10 | Employee Records |
| POL-001-PRO-11 | Payroll |
| POL-001-PRO-12 | Disciplinary |
| POL-001-PRO-13* | Supplier |

(*Where applicable)

## 27 COMMENCEMENT OF THE POLICY

This Policy shall be implemented with effect from the Senior Minister's date of approval and signature.

## 28 CONTACT DETAILS

| | |
|---|---|
| **Company Name:** | Shiloh Ministries NPC |
| **Information Officer:** | Pieter Theron |
| **Information Officer E-mail Address:** | administrator@shiloh.co.za |
| **Deputy Information Officer:** | N/A |
| **Deputy Information Officer E-mail Address:** | N/A |
| **Office Number:** | (012) 548-4200 |
| **Physical Address:** | 206 Hoefyster Singel, Roodeplaat |

| | | | |
|---|---|---|---|
| Shiloh MINISTRIES | Document Number | POL-001-FORM-04 | Rev 00 |
| | Document Title | Policy Acknowledgment Employee & Volunteer Declaration | |
| | Effective Date | | |
| | Review Date | | |

**Annexure A: Protection of Protected Information Act (POPIA) Policy Acknowledgment**

**POPIA Policy Acknowledgment & Employee Declaration**

By signing this document, I _____ hereby:

1. Confirm that I have received a copy of the POPI Policy and have been made aware of the contents as may be applicable and that I have been given the opportunity to refer any aspects that are unclear to me or questions I might have to the trainer or Information Officer.
2. Confirm that I have read the POPIA Policy and received adequate orientation on the POPIA Policy and such processes that affect my position and/or departmental operations in relation to POPIA.
3. Confirm that I will at all times adhere to the POPIA Policy and procedures of the Ministry.
4. Confirm that I am fully aware that the applicable and appropriate disciplinary action may follow if found in contravention and/or violation of this Policy.
5. Agree to report any breach with regards to this Policy to the Information Officer promptly and to comply with the policy and the procedures described therein.

Employee Name: _____

Employee Signature: _____

Date: _____

Information Officer (IO): _____

OI Signature _____

Date: _____

Instruction: Please file the duly executed declaration on the relevant employee file.

**Addendum B: Government Gazette Form 2**

**REQUEST FOR CORRECTION OR DELETION OF PROTECTED INFORMATION OR DESTROYING OR DELETION OF RECORD OF PROTECTED INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PROTECTED INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)**

**REGULATIONS RELATING TO THE PROTECTION OF PROTECTED INFORMATION, 2018**

[Regulation 3] *Note:*

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this form is inadequate, submit information as an Annexure to this form and sign each page.*
3. *Complete as is applicable.*

Request for (Mark the appropriate box with an "x"):

☐ Correction or deletion of the Protected Information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of Protected Information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record ofinformation.

| A | DETAILS OF THE DATA SUBJECT |
|---|---|
| Name(s) and surname / registered name of data subject: | |
| Unique identifier/ Identity Number: | |
| Residential, postal or business address: | |
| | |
| | Code ( ) |
| Contact number(s): | |
| E-mail address: | |
| **B** | **DETAILS OF RESPONSIBLE PARTY** |
| Name(s) and surname / | |

| | |
|---|---|
| registered name of responsible party: | |
| Residential, postal or business address: | |
| | |
| | Code ( ) |
| Contact number(s): | |
| E-mail address: | |
| **C** | **INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED** |
| | |
| | |
| | |
| **D** | **REASONS FOR *CORRECTION OR DELETION OF THE PROTECTED INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY. and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PROTECTED INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)* |
| | |
| | |
| | |
| | |

Signed at _____ this _____ day of _____ 20 _____.

_____*Signature of data subject/ designated person*