

PERSONAL INFORMATION PROTECTION WORKPLACE POLICY (POPI ACT WORKPLACE POLICY)

1. Introduction

1.1 Purpose

1.2 The Protection of Personal Information Act 4 of 2013 ("POPI") contains legal requirements relating to the collection, storing, handling, and processing of the Personal Information of certain persons.

1.3 The Organisation is involved in religious activities. The Organisation thus collects, stores, handles and processes the Personal Information as an integral part of its day-to-day activities.

1.3.1 As such, the purpose of this Policy is to:

1.3.1.1 ensure that the Organisation complies with all the applicable legal requirements and best practice for collecting, storing, handling and processing Personal Information of individuals;

1.3.1.2 protect employees' Personal Information; and

1.3.1.3 protect the Personal Information from unauthorised or unlawful disclosure or breach.

1.4 Scope

1.4.1 This Policy applies to all employees of the Organisation.

1.4.2 In addition, this Policy applies to all Personal Information processed by the Organisation and its employees.

2. Definitions

In this Policy:

2.1 "the Organisation" – means THE GOVERNING BODY OF THE APOSTOLIC FAITH MISSION OF SOUTH AFRICA (AFM) Westering ministering as "Crossroads Christian Fellowship";

2.2 "Data Subject" – means a person to whom Personal Information relates;

2.3 "Personal Information" – means personal information as defined in section 1 of POPI, namely information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

2.4 "Policy" – means this personal information protection workplace policy, as amended or replaced from time to time;

2.5 "processing" means any operation or activity concerning Personal Information;

2.6 "Processing Agreement" – means any personal information processing agreements concluded between the Organisation and persons from whom it receives Personal Information;

2.7 "Workplace" - means any premises or place where a person performs work.

3. Policy

3.1 A copy of this Policy will be made available to all employees and all employees are expected to familiarise themselves with the contents of this Policy.



3.2 This Policy hereby incorporates the terms and conditions of any Processing Agreements. As such, the Processing Agreements form an integral part of this Policy, and all employees are expected to familiarise themselves with the contents thereof and act in accordance therewith.

3.3 This Policy forms part of the employee's employment contract with the Organisation.

4. Principles of POPI

4.1 In order to become compliant with POPI and its legal requirements, there are eight principles that must be adhered to by the Organisation and its employees. These are:

- 4.1.1 Accountability;
- 4.1.2 Processing Limitation;
- 4.1.3 Purpose Specification;
- 4.1.4 Further Processing Limitation;
- 4.1.5 Information Quality;
- 4.1.6 Openness;
- 4.1.7 Security Safeguards; and
- 4.1.8 Data Subject Participation.

4.2 It is the responsibility of the employee to familiarise themselves with these principles as they are contained in POPI.

4.3 These principles and the rules of POPI apply regardless of how the Personal Information is collected or stored, whether on paper, digitally, or otherwise.

5. General Rules

5.1 At all times, Personal Information must be processed in accordance with all applicable laws, including but not limited to POPI, the rights of Data Subjects, and any Processing Agreements of the Organisation.

5.2 Personal Information may only be processed for the purposes of conducting the business of the Organisation and for no other purpose. If in doubt, employees should discuss with a more senior manager.

5.3 All Personal Information must remain strictly confidential and not be disclosed except in terms of POPI and any Processing Agreements.

5.4 Personal Information should not be transferred or otherwise exported for any reason without the prior consent of the Data Subjects concerned.

5.5 No more Personal Information should be collected than necessary for its purpose.

5.6 Personal Information should not be retained for longer than is reasonably necessary.

5.7 Personal Information may only be stored on approved data storage services.

5.8 Employees shall not save or make copies of the Personal Information for personal use.

5.9 All passwords used in respect of Organisation equipment and databases must be adequately strong.

6. Information Officer

The Organisation will appoint an Information Officer, as required by POPI, who will be responsible for your compliance under this Policy.

7. Data Subject Requests

From time to time, employees may be presented with requests from Data Subjects to access to rectify their Personal Information. Employees may provide such access with the oversight of a more senior person concerned only and should rectify such Personal Information strictly in accordance with the Data Subject's request.

8. Consequence of breaching this Policy

Should any employee breach this Policy, the Organisation shall take the necessary disciplinary action against that employee, and where should the employee be found in breach, he / she may be dismissed. This is without prejudice to any other rights and remedies the Organisation shall have in terms of applicable law.



It is the employee's responsibility to contact management should he/she have any queries.

