Southern Africa Philanthropy Foundation (SAPF)
Data Protection Policy
Presented for Board Approval

1. Purpose

The purpose of this policy is to ensure that SAPF processes all personal data lawfully, fairly, transparently, and in a manner that upholds the rights and dignity of individuals. This is in line with the **Protection of Personal Information Act (POPIA)** and other applicable data protection laws and best practices.

SAPF holds a duty of care to those we serve and works to safeguard personal and organisational data entrusted to us as part of our mission to advance dynamic and inclusive philanthropy in Southern Africa.

2. Scope of Application

This policy applies to:

- All SAPF staff, board members, volunteers, interns, and consultants
- All third-party vendors or partners who process personal data on SAPF's behalf

It covers all data held in digital or physical formats, including donor, grantee, partner, employee, and beneficiary information.

3. Our Commitment

SAPF commits to:

- Only collect and use personal data for legitimate, specified purposes
- Keep personal data secure, accurate, and up to date
- Ensure individuals understand how their data is used and protected
- Uphold the confidentiality and integrity of all data assets
- Respect the rights of data subjects to access, correct, or delete their information

4. Legal Framework

SAPF is guided by and compliant with the following:

- **Protection of Personal Information Act (POPIA)** – South Africa
- **General Data Protection Regulation (GDPR)** – where applicable to international partnerships
- Best practices in data ethics and nonprofit accountability

5. Key Definitions

- **Personal Information**: Any information that can identify an individual (e.g., name, ID number, contact details)
- **Data Subject**: The individual whose personal data is being collected
- **Processing**: Any operation performed on data (collection, storage, use, sharing, or destruction)
- **Responsible Party**: SAPF, which determines the purpose and means of data processing
- **Operator**: Any person or entity that processes data on SAPF's behalf

6. Principles of Data Processing

SAPF adheres to the following principles:

1. **Lawfulness and Fairness**: Process data in a lawful, reasonable, and transparent manner.
2. **Purpose Limitation**: Collect data only for specific, defined purposes.
3. **Data Minimisation**: Collect only data that is necessary and relevant.
4. **Accuracy**: Keep data accurate and up to date.
5. **Storage Limitation**: Retain data only for as long as necessary.
6. **Integrity and Confidentiality**: Protect data from loss, damage, or unauthorised access.
7. **Accountability**: Demonstrate compliance with data protection responsibilities.

7. Data Subject Rights

Under this policy, individuals have the right to:

- Be informed of how their data is used
- Access and request copies of their data
- Request correction, deletion, or restriction of data use
- Object to data processing for certain purposes
- Lodge complaints with the Information Regulator
- Requests must be directed to SAPF's **Information Officer** (see Section 11).

8. Data Security Measures

SAPF implements the following safeguards:

- Encrypted storage of digital data
- Access controls and password protection
- Secure disposal of physical records
- Staff training on data protection
- Contracts with data processors outlining confidentiality and security obligations

9. Third-Party Processing and Sharing

Personal data may only be shared with third parties:

- Where necessary for SAPF's operations or regulatory compliance
- Under written agreements that ensure POPIA-compliant protection
- With explicit consent from the data subject (where required)

10. Data Breach Response

In the event of a data breach:

- Immediate action will be taken to contain and investigate the breach
- Affected parties will be notified where required
- The Information Regulator will be informed of notifiable breaches
- Post-incident reviews will be conducted to prevent recurrence

11. Roles and Responsibilities

- **Board of Directors**: Provides oversight and ensures organisational accountability
- **CEO and Executive Management**: Enforces compliance and promotes a culture of data protection
- **Information Officer**: Oversees data management, responds to data requests, and liaises with regulators
- **All Staff**: Are responsible for handling data in accordance with this policy

12. Monitoring and Review

- This policy will be reviewed **every two years**, or in response to legal, operational, or technological changes
- Annual audits or spot-checks may be conducted to verify compliance

13. Policy Approval

Approved by the SAPF Board of Directors
Date of Approval: 1st of April 2025.

Signature of Board Chair: _____

Signature of CEO: _____

Next Review Date: 1st of April 2026.