

**POLICY ON THE PROTECTION OF PERSONAL INFORMATION ACT
04 OF 2013**

FOR

ACCESS TO INOVATIVE CARE FOUNDATION (“AICF”)

The Access to Innovative Care Foundation, (“AICF”) is a non-profit organisation established in December 2010 initially as the Innovative Cancer Care Foundation (ICCF) with the intent of improving patient access to innovative cancer care. In 2016, the ICCF expanded to incorporate other therapeutic areas where access to innovative care is a challenge for healthcare providers and patients and the name was changed to the AICF. The primary business of the AICF is to manage patient programmes that provide innovative care to eligible patients.

PREAMBLE

- A. The Protection of Personal Information Act 4 of 2013, (“POPIA/The Act”) and the Regulations promulgated in terms thereof require the Information Officer as defined under the Act to develop, implement, monitor and maintain a compliance framework, (Regulation 4 of Regulations published under GG number 42110 dated 14 December 2018).
- B. The purpose of the Act is to give effect to the Constitutional Right to privacy, by safeguarding personal information when processed by a responsible party subject to justifiable limitations.
- C. AICF is committed to complying with and promoting the spirit and purport of the Act.
- D. AICF recognizes and respects the right of Data Subjects to have their Personal Information protected as conferred by the Act.
- E. This Policy is hereby developed by AICF in compliance with the Act and Regulations in order to provide a compliance framework within which AICF, its officers and employees shall Process Personal Information.

F. AICF through this policy makes a commitment to protect the rights of Data Subjects as required by the Act various pieces of legislation that apply to the processing of personal information.

1. **SCOPE**

- 1.1. This policy applies to all AICF employees, officers, members, suppliers and the AICF Board and anyone who may process Personal Information for and on behalf of AICF.
- 1.2. The policy shall apply to all situations and business processes where Personal Information is processed, more importantly where such information may be made accessible to third parties.
- 1.3. The policy must be read together with the AICF PAIA Manual.
- 1.4 Forms 1 (Objection against processing), 2 (amendments to personal information) and 4 (Consent to electronic marketing) of the POPI Regulations are attached to this Policy.

2. **DEFINITIONS**

- 2.1. “**Applicable Legislation**” means all legislation applicable to AICF including POPI, National Archiving Act, Income Tax Act 58 of 1962; Value Added Tax Act 89 of 1991; Labour Relations Act 66 of 1995; Basic Conditions of Employment Act 75 of 1997; Employment Equity Act 55 of 1998; Skills Development Levies Act 9 of 1999; Unemployment Insurance Act 63 of 2001; Electronic Communications and Transactions Act 25 of 2002; Telecommunications Act 103 of 1996; Electronic Communications Act 36 of 2005; Consumer Protection Act 68 of 2008; National Credit Act 34 of 2005; and all legislation as listed under clause 7 of the AICF PAIA Manual.
- 2.2. “**Data Subject**” means the person to whom personal information relates as defined under the Act;
- 2.3. “**Employee**” means, for the purposes of this policy, any person employed permanently (full- or part-time), temporary, or on a fixed-term contract, and include contractors and AICF Board, that may come into contact with, use, process or otherwise deal with Personal Information.

- 2.4. **“Organisation”** means AICF and as the context indicates may also mean Employees and officers;
- 2.5. **“Operator”** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- 2.6. **“Personal information”** shall mean, for purposes of this policy and as defined under the Act, information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to:
- 2.6.1. information relating to the race, gender, sex, pregnancy, marital status, national,
 - 2.6.2. ethnic or social origin, colour, sexual orientation, age, physical or mental health,
 - 2.6.3. well-being, disability, religion, conscience, belief, culture, language and birth of the person;
 - 2.6.4. information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
 - 2.6.5. any identifying number, symbol or other particular assigned to the person;
 - 2.6.6. the address, fingerprints or blood type of the person;
 - 2.6.7. the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award of a prize to be made to another individual;
 - 2.6.8. 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;
 - 2.6.9. the views or opinions of another individual about the person;
 - 2.6.10. the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

- 2.6.11. the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
- 2.6.12. but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years.
- 2.6. **“Policy”** means this policy developed in terms of the Act and Regulations thereto;
- 2.7. **“Processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
 - 2.7.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - 2.7.2. dissemination by means of transmission, distribution or making available in any other form; or
 - 2.7.3. merging, linking, as well as restriction, degradation, erasure or destruction of information.
- 2.8. **“Purpose”** means the AICF’s purpose to Processing of Personal Information as set out under the Organisation’s PAIA Manual;
- 2.9. **“Special Personal Information”** means information relating to a person’s (a) religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) criminal behavior, as defined under the Act.
- 2.10. **“Responsible Party”** means, for purposes of this policy, all persons to whom this policy applies, whom, whether alone or in conjunction with others determines the purpose and means of processing Personal Information.

3. **AICF REQUIREMENTS FOR PROCESSING PERSONAL INFORMATION**

- A. All Processing of Personal Information must be done after a written and signed consent in a form developed and approved by the Organisation, has been received from the Data Subject.

- B. Where there is a legal requirement to disclose Personal Information to authorities, and consent is not required by law, the Data Subject must still be notified of such disclosure, unless the Applicable Law provides otherwise.

4. **CONDITIONS OF LAWFUL PROCESSING OF PERSONAL INFORMATION**

Section 4(1) of the Act requires that all Processing of Personal Information be done in a lawful manner. Anyone who Processes Personal Information for and on behalf the Organisation must do so in terms of the below conditions in order to ensure compliance with the Act:

- 4.1. Ensure that all the conditions and measures giving effect to conditions of the lawful processing of personal information as set out in the Act and this policy are complied with at the time of the determination of the purpose and means of the Processing and during the Processing.
- 4.2. Personal Information must only be processed with the consent of the Data Subject, for a specific, explicit and lawfully defined purpose, related to the functions and activities of AICF.
- 4.3. In the event of a requirement to use Personal Information outside the consented purpose, (“**further processing**”), then a further consent for the further processing must be obtained from the Data Subject prior to such further processing.
- 4.4. Personal Information must be collected directly from the Data Subject, should there be a need to collect the information from another source, the consent of the Data Subject must be obtained prior thereto.
- 4.5. Only up to date and correct Personal Information must be processed, and the Responsible Persons must ensure that the security measures put in place by AICF, as set out in the AICF PAIA Manual are used to secure the confidentiality and privacy of the Personal information.
- 4.6. No one should sell or make available the AICF databases for the distribution of any material without the Data Subjects’ consent.
- 4.7. Only relevant Personal Information required for the specified purpose should be collected- nothing in excess of that.

- 4.8. All communications of a marketing or general communications nature must be subject to an “opt out” functionality, which has to be adhered to strictly. The Data Subject’s consent for electronic marketing communications must be obtained on Form 4 as set out in the Regulations as amended in March 2025.
- 4.9. All requests for Personal Information and other information from any person or entity whatsoever shall be dealt with in accordance with the provisions of the AICF PAIA Manual and in line with this policy.
- 4.10. The Data Subject must be provided access to their Personal Information related upon written request and other request for access to personal and other information from any person or entity must be dealt with in terms of AICF PAIA Manual and in line with this policy.
- 4.11. All processing of Personal Information must immediately cease, in the event that the Data Subject withdraws its consent to the Processing or objects to the processing of Personal Information in the manner prescribed by law, except where AICF is by law obliged to continue such Processing.
- 4.12. Personal information must be corrected or deleted upon request by the data subject to do so, except where there is a legal or contractual obligation to retain.

5. SECURITY AND ACCESS

- 5.1. The Organisation uses the following security measures to secure Personal Information in its possession. Electronic information is secured by firewalls, cloud and data encryption and password secured access;

Access Level	Role	Type of Access Granted	Permitted Activities	Security Controls Applied
No Access	Visitors, external contractors (non-IT), general public	No access to Personal Information	None	N/A
Limited Read-Only Access	Specific Contracted Partners , - Insights	Read-only access to specific datasets. Restricted to patient information for a single program required to conduct	Viewing Personal Information and restricted	Unique user IDs, two-factor authentication, access limited to specific systems

Access Level	Role	Type of Access Granted	Permitted Activities	Security Controls Applied
		means testing services	uploads of results	AICF consultants will permit access to individual records in the dataset
Limited Read-Only Access	Board Members	Read-only access to information shared by Operation teams including, specific application queries, board minutes, foundation finances	Viewing information	Information sent via secure mail by Operation Team
Standard User Access	AICF Consultants, Operation team	Read and update Personal Information of patient applications relevant to assigned duties Access to information in the shared folders e.g. SOPs, training material, informed consents, program trackers, pharmaco-vigilance trackers, supporting information for applications, reports by program, program trackers	Capture, update, and maintain Personal Information View and contribute to information in the shared folder	Role-based access control, two-factor authentication to system Shared access folders, restricted to standard staff and shared by CEO
Operation Team Access	Senior management (CEO and Operations manager)	Access to broader datasets for oversight and reporting including, donor contracts, foundation finances, board minutes	Capture, update and maintain personal information. Monitoring, reporting, and approval functions	Role-based access control, two-factor authentication to system Shared access folders, restricted to operation team and shared by CEO
System Administrator Access	IT administrators	Full system access, including configuration and maintenance	System maintenance, backups, access provisioning, access to application information	Segregation of duties, enhanced logging, restricted administrative accounts

5.2. Anyone who requires access to Personal Information to fulfil the purposes of the Organisation and any legal obligations and under such circumstances where the information is legally required to be provided, is given access to the Personal Information;

5.3

5.4. The organisation shall notify the Data Subject in writing, should the Personal Information relating to the data subject be compromised or should there be a suspicion that the Personal Information is compromised.

6. STORAGE AND DESTRUCTION

6.1. All Personal Information in the possession of the Organisation must be stored, retained and destroyed in accordance with the legislation applicable to the specific information, according to AICF Policy / SOP on this matter.

6.2. Personal Information shall not be retained longer than required to fulfil the purpose for the Processing or longer than required by Applicable Legislation.

6.3. Once the purpose for Processing or the retention period provided under Applicable Legislation expires, the Personal Information must be destructed and/or deleted and/or returned to the Data Subject as may be required by Applicable Law and in a manner that complies with such Applicable Law.

7. COLLECTION OF PERSONAL INFORMATION

7.1 AICF collects Personal Information from various Data Subjects for varying purposes. E.g. Healthcare professional applying to the Organisation for funding on behalf of a patient. Such information must be collected in accordance with the provisions of the Act and this policy.

7.2 Only relevant Personal Information required for the specified purpose should be collected - nothing in excess of that. The data fields (see definition of “personal information” and “special information”) in all existing and new databases and types of information (e.g. contracts, financial information, marketing lists, etc.) will be evaluated as to whether that specific data field is:

7.2.1 Necessary, given the specific purpose for which the personal information will be used.

7.2. 2. Relevant for that purpose.

8. PURPOSE AND USE OF PERSONAL INFORMATION

8.1. When Processing Personal Information as part of any activity, the Responsible Party must:

8.1.1. Identify the nature and extent to which one will deal with (a) Personal Information and (b) Special Personal Information.

8.1.2. Identify the types of processing that will take place (e.g. collection, dissemination and destruction, or: collection, recording and storage, etc.).

8.1.3. Identify the purpose for which the specific processing is undertaken, clearly indicating whether such purpose is permitted by a law (e.g. invoicing requiring a VAT number).

8.1.4. Confirm that consent has been obtained from Data Subjects, which consent shall constitute a contract between the Organisation and the Data Subject and shall describe:

8.1.4.1. the purpose of the Processing or further processing of the Personal Information if any;

8.1.4.2. the type of Processing of the Personal Information;

8.1.4.3. timelines related to the Processing;

8.1.4.4. the destruction or storage of the Personal Information; and

8.1.5. Utilise the security assurances and measures undertaken by AICF to protect the data and Personal Information.

8.2. Information held by the Organisation

The Organisation holds information as set out under the AICF PAIA Manual and only for its purposes.

8.3. Personal information about children and special personal information

8.3.1. AICF does not process Personal Information about children except:

- 8.3.1.1. Upon prior consent of a legal guardian or parent or the child where applicable, or competent person as described in the Act;
- 8.3.1.2. If necessary for the establishment, exercise or defence of a right or obligation in law
- 8.3.1.3. If necessary to comply with an obligation of international public law
- 8.3.1.4. For historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- 8.3.1.5. If the Processing is of personal information which has deliberately been made public by the child with the consent of a competent person, or
- 8.3.1.6. Upon authorisation by the Information Regulator upon application and after publication in the Gazette and upon such conditions as may be imposed by the Information Regulator.

8.3.2. Special Personal Information must only be processed with Data Subject's consent or if otherwise as may be required by law.

8.4. Information shared by AICF

AICF will only share information with third parties:

- 8.4.1. upon the specific consent of the Data Subject and on written declaration that such third parties comply with the Act and related data legislation and regulations, or
- 8.4.2. if otherwise required to do so by any Applicable Law.

9. REVIEW AND AMENDMENT

This policy shall be reviewed every two years or more frequently as may be required and may be amended from time to time as may be required by law, for corrections of material errors, as the case may be.

10. TRAINING AND COMMUNICATION

All existing Employees, officers and AICF Board members and any person who may Process Personal Information for and on behalf of AICF shall be trained on an annual basis on this policy and underlying legal sources on which it is based. The training will also form part of new employee induction.

11. COMPLIANCE

11.1. The Information Officer shall maintain a report in relation to POPIA and PAIA regarding:

11.1.1. remedial steps taken in instances of non-compliance, including but not limited to:

11.1.1.1. Destruction of personal information;

11.1.1.2. De-identification of personal information;

11.1.1.3. Implementation of requisite security measures;

11.1.1.4. Implementation of access control measures;

11.1.1.5. Implementation of consents, contracts and policies or service level agreements within business activities and/or with third parties and contractors;

11.1.1.6. Disciplinary action against employees violating this policy;

11.1.1.7. The submission of regular progress reports;

11.1.1.8. Obtaining expert assistance, where required; and

11.1.1.9. Undergoing of training on POPIA and PAIA of designated staff.

12. INFORMATION OFFICE

12.1. The following may be directed to the Information Officer in writing to jeanette@AICF.org.za

12.1.1. Complaints

Any complaints by any person including, employees, third parties, Board members on any violation of this policy or data privacy.

12.1.2. Objections, withdrawals, amendments and deletions

12.1.2.1. Any objections to processing of personal information, withdrawal of consents, requests to amend or delete Personal Information.

12.2. Objections, requests for withdrawals, amendments and deletions must be made on the forms as provided for in the Regulations published under GG number 42110 dated 14 December 2018 and amended in 2025, which forms shall be made available on our website.