DHS Foundation Trust Protection of Personal Information Policy

1. Legal Background

The right to privacy is an integral human right recognized and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (POPI). POPI aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

As a result of its operations, the DHS Foundation Trust ("DHSFT") is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of donors, trustees, employees, and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, DHSFT is committed to effectively manage personal information in accordance with POPI's provisions.

2. Definitions

2.1 Personal Information

Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, believe, culture, language, and birth of a person;
- information relating to the education or medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
- the biometric information of the person;
- personal opinions, views, or preferences of the person;
- 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;
- the view or opinions of another individual about the person;
- 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.

2.2 Data Subject

This refers to the natural or juristic person to whom personal information relates, such as a donor, trustee, employee, director, or a company that supplies DHSFT with products or other goods and services.

2.3 Responsible Party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case DHSFT is the responsible party.

2.4 Operator

An operator means a person who processes personal information for DHSFT in terms of a contract or mandate, without coming under the direct authority of DHSFT. For example, a third-party service provider that has contracted with DHSFT to shred documents containing personal information or provide IT related

services. When dealing with an operator, the contract or mandate regulating the relationship between the parties should include an indemnity clause.

2.5 Information Officer

The Information Officer is responsible for ensuring DHSFT's compliance with POPI. The CEO of DHSFT is responsible for performing the Information Officer's duties. He may delegate his responsibilities in this regard to various Deputy Information Officers throughout the DHSFT.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

Means any recorded information, regardless of from or medium, including:

- writing on any material;
- information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- book, map, plan, graph, or drawing;
- photograph, film, negative, tape or other device 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.

2.8 Filing System

Means any structured set of personal information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

Means any identifier that is assigned to a data subject and is used by DHSFT for the purposes of its operations and that uniquely identifies that data subject in relation to DHSFT.

2.10 De-Identify

This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- promoting or updating, in the ordinary course of business, any new developments to the data subject;
- requesting the data subject to make a donation for any kind for any reason.

2.14 Biometrics

Means a technique of personal identification that is based on physical, physiological, or behavioural characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. Policy Purpose

The purpose of this policy is to protect DHSFT from the compliance risks associated with the protection of personal information which includes:

- **Breaches of confidentiality**
  For instance, DHSFT could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately;

- **Failing to offer choice**
  For instance, all data subjects should be free to choose how and for what purpose DHSFT uses information relating to them.

- **Reputational damage**
  For instance, DHSFT could suffer a decline in donations following an adverse event such as a computer hacker deleting the personal information held by DHSFT.

  This policy demonstrates DHSFT's commitment to protect the privacy rights of data subjects in the following manner:

  - through stating desired behaviour and directing compliance with the provisions of POPI and best practice;
  - by cultivating an organisational culture that recognises privacy as a valuable human right;
  - by developing and implementing internal controls for the purpose of managing compliance risk associated with the protection of personal information;
  - by creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of DHSFT;
  - by assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer as well as Deputy Information Officers in order to protect the interests of DHSFT and data subjects;
  - by raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. Policy Application

The policy and its guiding principles apply to:

- DHSFT's board of trustees and executives
- All operations of DHSFT;

- All employees;
- All contractors, suppliers, consultants, agents, and other persons acting on behalf of DHSFT.

The policy's guiding principles find application in all situations and must be read in conjunction with POPI as well as DHSFT's PAIA Policy.

The legal duty to comply with POPI's provisions is activated in any situation where there is:

A PROCESSING of PERSONAL INFORMATION entered into a RECORD by or for DHSFT

POPI does not apply in situations where the processing of personal information:

- Concluded in the course of purely personal or household activities, or
- Where the personal information has been de-identified.

5. Rights of Data Subjects

Where appropriate, DHSFT will ensure that its trustees, employees, and agents are made aware of the rights conferred upon them as data subjects.

DHSFT will ensure that it gives effect to the following seven rights:

5.1 The Right to Access Personal Information

DHSFT recognizes that a data subject has the right to establish whether DHSFT holds personal information relating to him, her, or it, including the right to request access to that personal information. A "**Personal Information Request Form**" can be found under Annexure A.

5.2 The Right to have Personal Information Corrected or Deleted

The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where DHSFT is no longer authorised to retain personal information.

5.3 The Right to Object to the Processing of Personal Information

The data subject has the right, on reasonable grounds, to object to the processing of his, hers or its personal information. In such circumstances, DHSFT will give due consideration to the request and the requirements of POPI. The organization may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of personal information.

5.4 The Right to Object to Direct Marketing

The data subject has the right to object to the processing of his, hers or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Complain to the Information Regulator

The data subject has the right to submit a complaint to the Information Regulator regarding the alleged infringement of any of the rights protected under POPI and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information. An example of a "**POPI Complaint Form**" can be found under Annexure B.

5.6 The Right to be Informed

The data subject has the right to be notified that his, her or its personal information is being collected by DHSFT. The data subject has the right to be notified in any situation where DHSFT has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. General Guiding Principles

All employees and persons acting on behalf of the DHSFT will always be subject to, and act in accordance with the following guiding principles:

6.1 Accountability

Failing to comply with POPI could potentially damage DHSFT's reputation or expose DHSFT to a civil claim for damages. The protection of information is therefore everybody's responsibility.

DHSFT will ensure that the provisions of POPI and guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, DHSFT will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Process Limitation

DHSFT will ensure that personal information under its control is processed:

- in a fair, lawful, and non-excessive manner,
- only with the informed consent of the data subject, and
- only for a specifically defined purpose.

DHSFT will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

DHSFT will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiaries) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

Where applicable, the data subject must be informed of the possibility that their personal information will be shares with other aspects of DHSFT's business and be provided with reasons for doing so.

An example of a "POPI Notice and Consent Form" can be found under Annexure C.

6.3 Purpose Specification

All of DHSFT's businesses and operations must be informed by the principle of transparency.

DHSFT will process personal information only for specific, explicitly defined, and legitimate reasons. DHSFT will inform data subjects of these reasons prior to collecting or recording the data subjects' personal information.

6.4 Further Processing Limitation

Personal information will not be processed for a secondary purpose unless the processing is compatible with the original purpose.

Therefore, where DHSFT seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where the secondary purpose is not compatible with the original purpose, DHSFT will first obtain additional consent from the data subject.

6.5 Information Quality

DHSFT will take reasonable steps to ensure that all information collected is complete, accurate and not misleading. Where personal information is collected from third parties, DHSFT will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly from the data subject or by way of independent resources.

6.6 Open Communication

DHSFT will take reasonable steps to ensure that the data subjects are notified that their personal information is being collected including the purpose for which it is being collected and processed. DHSFT established and maintains a "contact us" facility on its website (www.dhsfoundation.co.za) for data subjects who wants to:

- enquire whether DHSFT holds related personal information;
- request access to related personal information;
- request DHSFT to update or correct related personal information;
- make a complaint concerning the processing of personal information.

6.7 Security Safeguards

- DHSFT will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimize the risk of loss, unauthorized access, disclosure, interference, modification, or destruction.

- Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

- DHSFT will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on DHSFT's IT network.

- DHSFT will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorized individuals.

- All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which DHSFT is responsible.

- All existing employees will, after the required consultation process had been followed, be required to sign an addendum to their employment contract containing the relevant consent and confidentiality clauses.

- DHSFT's suppliers and third-party service providers will be required to enter into a service level agreement with DHSFT where both parties pledge their mutual commitment to POPI and the lawful processing of any personal information pursuant to the agreement.

- An example of "Employee Consent and Confidentiality Clause" for inclusion in DHSFT's employment contracts can be found under Annexure D.

- An example of an "SLA Confidentiality Clause" for inclusion in DHSFT's service level agreement can be found under Annexure E.

6.8 Data Subject Participation

A data subject may request the correction or deletion of his, her or its personal information held by DHSFT.

DHSFT will ensure that it provides a facility for data subjects who wants to request the correction or deletion of their personal information.

Where applicable, DHSFT will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. Information Officers

DHSFT's Information Officer is the CEO. He may appoint Deputy Information Officers in each of DHSFT's businesses and delegate to them the responsibility for ensuring compliance with POPI.

The Information Officer as well as any Deputy Information Officers will be registered with the South African Information Regulator established under POPI.

8. Specific Duties and Responsibilities

8.1 DHSFT Board of Trustees

DHSFT's board of trustees is ultimately answerable for ensuring that DHSFT meets its legal obligations in terms of POPI.

The DHSFT board has delegated its responsibilities in terms of POPI to management and the Information Officer and Deputy Information Officers.

The DHSFT board is responsible for ensuring that:

- All persons responsible for the processing of personal information on behalf of DHSFT:
  - are appropriately trained and supervised to do so;
  - understand that they are contractually obligated to protect the personal information they come into contact with; and
  - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of periodic POPI Audits in order to accurately access and review the ways in which DHSFT collects, holds, uses, shares, discloses, destroys and process personal information.

8.2 Information Officer/Deputy Information Officers

These officers are responsible for:

- Taking steps to ensure DHSFT's reasonable compliance with POPI.
- Keeping DHSFT board updated about DHSFT's information protection responsibilities under POPI. For instance, in the case of a security breach, the Information Officer must inform and advise the DHSFT Board of their obligations pursuant to POPI;

- Continually analysing privacy regulations and aligning them with DHSFT's personal information processing procedures. This will include DHSFT's information protection procedures and related policies;
- Ensuring POPI audits are scheduled;
- Ensuring DHSFT makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to DHSFT;
- Approving any contracts entered into with employees and other third parties which may have an impact on the personal information held by DHSFT;
- Encouraging compliance with the conditions required for the lawful processing of personal information;
- Ensuring that employees and other persons acting on behalf of DHSFT are fully aware of the risks associated with the processing of personal information and that they remain informed about DHSFT's security controls;
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of DHSFT;
- Addressing employees' POPI related questions;
- Addressing all POPI related requests and complaints by DHSFT's data subjects;
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officer/ Deputy Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

8.4 Chief executive (or appropriate person with required authority from the CEO)

The chief executive/ or appropriately authorised person is responsible for:

- Approving the protection of personal information statements and disclaimers that are displayed on DHSFT's website, including those attached to communications such as emails.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of DHSFT to ensure that any outsourced initiatives comply with POPI.

8.5 Employees and other Persons acting on behalf of DHSFT

Employees and other persons acting on behalf of DHSFT will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of DHSFT are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of DHSFT may not directly or indirectly utilise, disclose or make public in any manner to any person or third party, either within DHSFT or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of DHSFT must request assistance from the appropriate director or Deputy Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of DHSFT will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing is necessary for pursuing the legitimate interests of DHSFT or of a third party to whom the information is supplied.

Furthermore, personal information will only be processes where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected;
- Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

Consent to process a data subjects' personal information will be obtained directly from the data subject, except where:

- The personal information has been made public; or
- Where valid consent has been given to a third party; or
- The information is necessary for effective law enforcement.

Employees and other persons acting on behalf of DHSFT will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties;
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from DHSFT's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure.
- Transfer personal information outside the borders of South Africa without the permission from the Information Officer.

Employees and other persons acting on behalf of DHSFT are responsible for:

- Keeping all personal information that they come into contact with, secure by taking sensible precautions and following guidelines as outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to a printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant director or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of DHSFT, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or a Deputy Information Officer.

9. POPI Audit

DHSFT's Information Officer may schedule periodic POPI Audits.

The purpose of a POPI audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout DHSFT. For instance, DHSFT's various business units and divisions.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage DHSFT's POPI related compliance risk.

In performing the POPI Audit, Information Officers will liaise with employees in order to identify areas within in DHSFT's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

Information Officers will be permitted direct access to and have demonstrable support from employees and DHSFT's governing body in performing their duties.

10. Request to Access Personal Information Procedure

Data subjects have the right to:

- Request what personal information DHSFT holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against DHSFT's PAIA Policy.

The Information Officer will process all requests within a reasonable time.

11. POPI Complaints Procedure

- Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The organisation takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:
- POPI complaints must be submitted to DHSFT in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form".
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on DHSFT's data subjects.
- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with DHSFT's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to DHSFT's governing body within 7 working days of receipt of the complaint. In all instances, DHSFT will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
    - A suggested remedy for the complaint,
    - A dismissal of the complaint and the reasons as to why it was dismissed,
    - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
    - Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
    - The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

12. Disciplinary Action

Where a POPI complaint or a POPI infringement investigation has been finalised, DHSFT may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, the organisation will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the organisation may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.