



# HARVARD HOUSE

## **PROTECTION OF PERSONAL INFORMATION ACT**

### **POLICY MANUAL**



## APPROVAL

---

Any reference to the “Group” shall refer to the “Harvard House Group” which comprises the following legal entities:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd \*\*
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust \*\*
- Harvard House Insurance Brokers (Pty) Ltd \*\*

*\*\* Authorised Financial Service Provider*

This policy forms part of the Group’s internal business processes and procedures.

The board of directors, employees, service providers and any other persons acting on behalf of the Group are required to familiarise themselves with the policy’s requirements and undertake to comply with the stated processes and procedures.

This policy has been approved as follows:

Approver	Role	Signature	Date
Peter Smith	Chief Executive Officer		
Collen Rees	Compliance Liaison Officer		
Robert Pool	Group Business Analyst		

## CONTROL PROCEDURES AND ACTIVITIES

---

- Implement internal controls that will provide reasonable assurance that the Group’s compliance obligations are met and that non-compliances are prevented, detected and corrected.
- Internal controls must be periodically evaluated and tested to ensure their continuing effectiveness.

Activity	Control Owner
Annual Review of Policy	Robert Pool
Information Officer	Robert Pool
Deputy Information Officer	Dot Humphries
POPIA Audit	Robert Pool
POPIA Awareness Training	Robert Pool





## CONTENTS

---

	Page
1. INTRODUCTION.....	4
2. DEFINITIONS.....	4
3. POLICY PURPOSE .....	6
4. POLICY APPLICATION .....	7
5. RIGHTS OF DATA SUBJECTS .....	7
5.1. The Right to Access Personal Information.....	7
5.2. The Right to have Personal Information Corrected or Deleted .....	7
5.3. The Right to Object to the Processing of Personal Information .....	8
5.4. The Right to Object to Direct Marketing.....	8
5.5. The Right to Complain to the Information Regulator.....	8
5.6. The Right to be Informed .....	8
6. GENERAL GUIDING PRINCIPLES .....	8
6.1. Accountability .....	8
6.2. Processing Limitation .....	8
6.3. Purpose Specification .....	9
6.4. Further Processing Limitation .....	9
6.5. Information Quality .....	9
6.6. Open Communication .....	9
6.7. Security Safeguards.....	10
6.8. Data Subject Participation .....	10
7. INFORMATION OFFICERS.....	10
8. SPECIFIC DUTIES AND RESPONSIBILITIES.....	11
8.1. Board of Directors .....	11
8.2. Information Officer.....	11
8.3. IT Manager .....	12
8.4. Marketing Manager .....	12
8.5. Employees and Other Persons Acting on Behalf of the Group.....	13
9. POPIA AUDIT.....	15
10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE .....	15
11. POPIA COMPLAINTS PROCEDURE.....	16
12. DATA BREACH MANAGEMENT .....	16
13. DISCIPLINARY ACTION.....	18





## 1. INTRODUCTION

---

In terms of the Protection of Personal Information Act of 2013 (“POPIA”), any responsible party that processes personal information must do so in accordance with the principles outlined in POPIA.

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act.

POPIA 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.

Through the provision of quality goods and services, the organisation is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, 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, the organisation is committed to effectively managing personal information in accordance with POPIA'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, belief, culture, language and birth of a person;
- information relating to the education or the 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;
- the 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 views 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 an individual client, or a company that supplies the Group with products or other goods.





### **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, the Group is the responsible party.

### **2.4. Operator**

An 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. For example, a third-party service provider that has contracted with the Group to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

### **2.5. Information Officer**

The Information Officer is responsible for ensuring the Group's compliance with POPIA.

Where no Information Officer is appointed, the head of the Group will be responsible for performing the Information Officer's duties.

Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

### **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, organisation, 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 form 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 centralised, decentralised 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 a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject for the responsible party.

## **2.10. De-Identify**

Means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify a data subject, 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 offering to supply, in the ordinary course of business, any goods or services to the data subject; or
- requesting the data subject to make a donation of any kind for any reason.

## **2.14. Biometrics**

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

# **3. POLICY PURPOSE**

---

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

- breaches of confidentiality, eg. the Group 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, eg. all data subjects should be free to choose how and for what purpose the Group uses information relating to them,
- reputational damage, eg. the Group could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the Group.

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

- through stating desired behaviour and directing compliance with the provisions of POPIA and best practice,
- by cultivating a Group culture that recognises privacy as a valuable human right,





- by developing and implementing internal controls for the purpose of managing the 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 the Group,
- by assigning specific duties and responsibilities, including the appointment of an Information Officer and, where necessary, Deputy Information Officers in order to protect the interests of the Group 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

---

This policy and its guiding principles apply to:

- the Group's board of directors,
- all legal entities, departments and branches of the Group,
- all employees and volunteers,
- all contractors, service providers and other persons acting on behalf of the Group.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the Group's PAIA Policy as required by the Promotion of Access to Information Act.

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 a responsible person who is domiciled in South Africa.

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

- is 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, the Group will ensure that its clients are made aware of the rights conferred upon them as data subjects.

The Group will ensure that it gives effect to the following six rights.

### 5.1. The Right to Access Personal Information

The Group recognises that a data subject has the right to establish whether the Group holds personal information related to him, her or it including the right to request access to that personal information.

An example of 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 the Group is no longer authorised to retain the 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, her or its personal information.

In such circumstances, the Group will give due consideration to the request and the requirements of POPIA. The Group 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 the personal information.

### **5.4. The Right to Object to Direct Marketing**

The data subject has the right to object to the processing of his, her 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 an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

An example of a "POPIA 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 the Group.

The data subject also has the right to be notified in any situation where the Group 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 Group will at all times be subject to, and act in accordance with, the following guiding principles:

### **6.1. Accountability**

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

The Group will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the Group will take appropriate actions, 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. Processing Limitation**

The Group 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.







The Group 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. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the Group will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

The Group will under no circumstances distribute or share personal information between separate legal entities, associated entities (such as subsidiary companies) 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 shared with other aspects of the Group's business and be provided with the reasons for doing so.

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

### **6.3. Purpose Specification**

All of the Group's business units and operations must be informed by the principle of transparency.

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

### **6.4. Further Processing Limitation**

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

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

### **6.5. Information Quality**

The Group will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. The more important it is that the personal information be accurate, the greater the effort the Group will put into ensuring its accuracy.

Where personal information is collected or received from third parties, the Group will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

### **6.6. Open Communication**

The Group will take reasonable steps to ensure that data subjects are notified or are always aware that their personal information is being collected including the purpose for which it is being collected and processed.

The Group will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

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





## **6.7. Security Safeguards**

The Group will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

Security measures also need to be applied in a context-sensitive manner. The more sensitive the personal information, the greater the security required.

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

The Group will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised 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 the Group is responsible.

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

The Group's operators and third-party service providers will be required to enter into service level agreements with the Group where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

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

An example of an "SLA Confidentiality Clause" for inclusion in the Group's service level agreements 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 the Group.

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

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

# **7. INFORMATION OFFICERS**

---

The Group will appoint an Information Officer and, where necessary, a Deputy Information Officer to assist the Information Officer.

The Group's Information Officer is responsible for ensuring compliance with POPIA.

There are no legal requirements under POPIA for a Group to appoint an Information Officer. Appointing an Information Officer is, however, considered to be a good business practice, particularly within larger Groups.

Where no Information Officer is appointed, the head of the Group will assume the role of the Information Officer.





Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

Once appointed, the Group will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

An example of an “Information Officer Appointment Letter” can be found under Annexure F.

## 8. SPECIFIC DUTIES AND RESPONSIBILITIES

---

### 8.1. Board of Directors

The Group’s board of directors cannot delegate its accountability and is ultimately answerable for ensuring that the Group meets its legal obligations in terms of POPIA.

The board of directors may, however, delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The board of directors is responsible for ensuring that:

- the Group appoints an Information Officer and, where necessary, a Deputy Information Officer,
- all persons responsible for the processing of personal information on behalf of the Group:
  - 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 enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so,
- the scheduling of a periodic POPIA Audit in order to accurately assess and review the ways in which the Group collects, holds, uses, shares, discloses, destroys and processes personal information.

### 8.2. Information Officer

The Group’s Information Officer is responsible for:

- Taking steps to ensure the Group’s reasonable compliance with the provisions of POPIA.
- Keeping the board of directors updated about the Group’s information protection responsibilities under POPIA. In the case of a security breach, the Information Officer must inform and advise the board of directors of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the Group’s personal information processing procedures. This will include reviewing the Group’s information protection procedures and related policies.
- Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
- Ensuring that the Group makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the Group. For instance, maintaining a “contact us” facility on the Group’s website.





- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the Group. This will include overseeing the amendment of the Group's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the Group are fully aware of the risks associated with the processing of personal information and that they remain informed about the Group's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the Group.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the Group's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officer 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.

### **8.3. IT Manager**

The Group's IT Manager is responsible for:

- ensuring that the Group's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards,
- ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services,
- ensuring that servers containing personal information are sited in a secure location, away from the general office space,
- ensuring that all electronically stored personal information is backed-up and tested on a regular basis,
- ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts,
- ensuring that personal information being transferred electronically is encrypted,
- ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software,
- performing regular IT audits to ensure that the security of the Group's hardware and software systems are functioning properly,
- performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons,
- performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the Group's behalf.

### **8.4. Marketing Manager**

The Group's Marketing Manager is responsible for:

- approving and maintaining the protection of personal information statements and disclaimers that are displayed on the Group's website, including those attached to communications such as emails and electronic newsletters.
- addressing any personal information protection queries from journalists or media outlets such as newspapers.





- where necessary, working with persons acting on behalf of the Group to ensure that any outsourced marketing initiatives comply with POPIA.

### **8.5. Employees and Other Persons Acting on Behalf of the Group**

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

Employees and other persons acting on behalf of the Group 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 the Group may not directly or indirectly, use, disclose or make public in any manner to any person or third party, either within the Group 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 the Group must request assistance from their managers or the 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 the Group will only process personal information where:

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

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

- clearly understands why and for what purpose his, her or its personal information is being collected, and
- has given the Group written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the Group will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the Group will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's 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 the Group 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 the Group's central database or a dedicated server,
- share personal information informally. Personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant manager or the Information Officer,
- transfer personal information outside of South Africa without the express permission from the Information Officer.

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

- keeping all personal information that they come into contact with secure, by taking precautions and following the guidelines 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 Group, 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,
- 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 such as a locked drawer of a filing cabinet,
- ensuring that where personal information has been printed, that the paper printouts are not left unattended where unauthorised individuals could see or copy them,
- taking reasonable steps to ensure that personal information is kept accurate and up to date by confirming a data subject's contact details when the client 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 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 manager or the Information Officer to delete or dispose of the personal information in the appropriate manner,
- undergoing POPIA Awareness training from time to time.





Where an employee, or a person acting on behalf of the Group, 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 the Deputy Information Officer.

## 9. POPIA AUDIT

---

The Group's Information Officer will schedule periodic POPIA Audits.

The purpose of a POPIA audit is to:

- identify the processes used to collect, record, store, disseminate and destroy personal information,
- determine the flow of personal information throughout the Group's various legal entities, departments, branches and other associated entities,
- 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 extent of compliance with POPIA and this policy,
- monitor the effectiveness of internal controls established to manage the Group's POPIA related compliance risk.

In performing the POPIA Audit, the Information Officer will liaise with managers in order to identify areas within the Group's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

The Information Officer will be permitted direct access to and have demonstrable support from managers and the Group's board of directors in performing his or her duties.

## 10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

---

Data subjects have the right to:

- request what personal information the Group 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 the Group's PAIA Policy.

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







## 11. POPIA COMPLAINTS PROCEDURE

---

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed. The Group takes all complaints seriously and will address all POPIA related complaints in accordance with the following procedure:

- POPIA complaints must be submitted to the Group in writing. Where so required, the Information Officer will provide the data subject with a “POPIA 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 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 the Group’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 the Group’s board of directors 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 the Group’s board of directors within 7 working days of receipt of the complaint. In all instances, the Group 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 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 POPIA related complaints.

## 12. DATA BREACH MANAGEMENT

---

A data breach means any event or action which may compromise the confidentiality, integrity or availability of the Group’s systems or data, which caused or has the potential to cause loss or damage to the Group.

A data breach includes but is not limited to:

- theft or loss of personal information,
- theft or loss of equipment which contains personal information, irrespective of whether the equipment is owned by the Group. Equipment refers to any physical object that contains or stores







data and/or personal information which includes, but is not limited to, computers, laptops, USBs, tablets, cellphones and paper records,

- failure of Group systems and/or equipment,
- unauthorised use of, access to or modification of Group data or systems,
- unauthorised disclosure of personal information,
- unauthorised access or attempted unauthorised access to Group systems and/or personal information.

The responsibility to report any data breach or information security incident, whether confirmed or suspected, vests with the employees, contractors, service providers and other persons acting on behalf of the Group who access, use or manage the data of the Group.

Data breaches and information security incidents need to be reported immediately to the Information Officer.

Any data breach or information security incident reported will be investigated by the Information Officer who will:

- contain the breach,
- assess the potential adverse consequences,
- limit the scope and impact of the breach,
- determine a suitable cause of action to ensure a resolution to the incident.

Should any personal information be disclosed without authorisation, whether or not the disclosure was intentional, the following process will be followed:

- the recipient will be advised that the information cannot be distributed or discussed with anyone else, and the implications of the failure to do so will be explained to the recipient,
- the recipient will be advised to destroy or delete the information, and written confirmation will be requested as confirmation that the information has been destroyed or deleted as required,
- where required, the data subjects will be informed of the unauthorised disclosure in order to take any steps available to protect themselves.

The Information Officer will immediately, or as soon as may be reasonably possible, investigate any data breach or information security incident reported and assess the risk associated with it taking into account:

- the type of data involved,
- the sensitivity of the data,
- the data protection currently utilised, such as encryptions,
- what happened to the data, whether it was lost, stolen or damaged,
- whether the data can be utilised for illegal means ,
- the data subjects affected by the incident or breach, the number of individuals involved and the potential effects on the data subjects,
- the wider consequence of the breach, if any,
- manner in which losses can be recovered and the damage caused limited.

The Information Officer is responsible for all notifications required in terms of this policy, which includes any notification to the Information Regulator, as required in terms of POPIA, data subjects or third parties.





In the event that the severity of the data breach or information security incident requires notification to the data subjects, the data subjects will be informed as soon as may be reasonably possible in order to mitigate any damage or possible damage that may occur to the data subjects. Notifications to data subjects will include:

- a description of the breach or incident,
- the manner in which the breach or incident occurred,
- when the breach occurred,
- the data involved in the breach or incident,
- recommendation on how to mitigate any further damage or loss,
- the action taken by the Group to mitigate the risks,
- the contact information of the Information Officer.

The Group will maintain a record of all data breaches and information security incidents, regardless of whether any further notification was required.

Upon containment of any breach or incident, the Information Officer will review the causes of the breach, the effectiveness of the response and whether any system changes or policy or procedures amendments should be implemented.

The existing controls will be reviewed to determine adequacy and corrective action will be implemented to minimise the risk of similar incidents.

The review will consider:

- the manner in which personal data is collected and stored,
- the potential risks existing within existing security measures,
- the security of transmissions,
- staff awareness.

### 13. DISCIPLINARY ACTION

---

Where a POPIA complaint or a POPIA infringement investigation has been finalised, the Group 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 in this policy.

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

Any gross negligence or the intentional mismanagement of personal information, will be considered a serious form of misconduct for which the Group 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.



# PERSONAL INFORMATION REQUEST FORM



## HARVARD HOUSE

We understand your need for  
FINANCIAL INTEGRITY

### PRELUDE

Please submit the completed form to the Information Officer:

Full Name: Robert James Pool

Contact Number: 033 330 2164

Email Address: [robertp@hhgroup.co.za](mailto:robertp@hhgroup.co.za)

Please be aware that you may be required to provide proof of identification prior to us processing your request.

There may also be a reasonable charge for providing copies of the information requested.

### PARTICULARS OF DATA SUBJECT

Title Initials

Surname

First Name(s)

ID Number

Telephone Mobile

Email

#### Postal Address

c/o

Building

Street

Suburb

City

Postal Code

### REQUEST

I request the Group to:

Confirm whether it holds any of my personal information.

Provide a record or description of my personal information.

Correct or update my personal information.

Destroy or delete a record of my personal information.

#### The Harvard House Group:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd \*\*
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust \*\*
- Harvard House Insurance Brokers (Pty) Ltd \*\*

\*\* Authorised Financial Service Provider

## INSTRUCTIONS

## AUTHORISATION

**Signature**

**Date**



# POPIA COMPLAINT FORM



## HARVARD HOUSE

We understand your need for  
FINANCIAL INTEGRITY

### PRELUDE

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act of 2013.

Please submit your complaint to the Information Officer:

Full Name: Robert James Pool  
Contact Number: 033 330 2164  
Email Address: [robertp@hhgroup.co.za](mailto:robertp@hhgroup.co.za)

Where we are unable to resolve your complaint to your satisfaction you have the right to complain to the Information Regulator:

The Information Regulator: Ms Mmamoroke Mphelo  
Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria  
Email: [inforreg@justice.gov.za](mailto:inforreg@justice.gov.za)  
Telephone: 012 406 4818

### PARTICULARS OF COMPLAINANT

Title	Initials
Surname	
First Name(s)	
ID Number	
Telephone	Mobile
Email	
<b>Postal Address</b>	
c/o	
Building	
Street	
Suburb	
City	
Postal Code	

#### The Harvard House Group:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd \*\*
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust \*\*
- Harvard House Insurance Brokers (Pty) Ltd \*\*

\*\* Authorised Financial Service Provider

## DETAILS OF COMPLAINT

## DESIRED OUTCOME

## AUTHORISATION

**Signature**

**Date**



# POPIA NOTICE AND CONSENT FORM



**HARVARD  
HOUSE**

We understand your need for  
FINANCIAL INTEGRITY

## PRELUDE

The Constitution of the Republic of South Africa provides that everyone has the right to privacy and the Protection of Personal Information Act 4 of 2013 ("POPIA") includes the right to protection against unlawful collection, retention, dissemination and use of personal information.

Any reference to the "Group" shall refer to the "Harvard House Group" which comprises the following legal entities:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust
- Harvard House Insurance Brokers (Pty) Ltd

The Group is committed to protecting your privacy and recognises that it needs to comply with statutory requirements in collecting, processing, storing and sharing of personal information. In terms of section 18 of POPIA, if personal information is collected, the Group, as the responsible party, must take reasonably practical steps to ensure that the data subject is made aware of:

- the purpose for processing the information,
- the type of information being collected,
- whether the information will be shared with any third parties,
- the right to access and amend the information,
- the right to object to the processing of the information.

For further information, please refer to the Group's POPIA Policy Manual which can be accessed on our website ([www.hhgroup.co.za](http://www.hhgroup.co.za)) or by contacting the Information Officer:

- Full Name: Robert James Pool
- Contact Details: 033 330 2164 or [robertp@hhgroup.co.za](mailto:robertp@hhgroup.co.za)

## PURPOSE FOR PROCESSING INFORMATION

The Group collects, processes, stores and shares your personal information primarily to provide you with access to the Group's services and products. The Group will only process your information for a purpose you would reasonably expect, including, but not limited to:

- providing you with financial advice, services and products that suit your needs as requested,
- issue, administer and manage investments,
- keep you informed of the latest financial news and market updates,
- prepare financial statements and submit tax returns,
- conduct estate planning and draft wills,
- obtain insurance quotes and process claims,
- comply with any legal and regulatory requirements.

### The Harvard House Group:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd \*\*
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust \*\*
- Harvard House Insurance Brokers (Pty) Ltd \*\*

\*\* Authorised Financial Service Provider

## TYPE OF INFORMATION BEING COLLECTED

Some of your information that the Group collects may include your full name, title, identity number, date of birth, contact numbers, email address, postal and physical address, tax number, residency status, employment status, occupation, investments, assets, liabilities, income, expenditure, banking details, insurance policies and family history.

## SHARING OF INFORMATION WITH THIRD PARTIES

The Group may need to share your information to provide advice, reports, analyses, services or products that you have requested. Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

## THE RIGHT TO ACCESS AND AMEND INFORMATION

You have the right to access and amend your personal information at any reasonable time by completing and submitting a Personal Information Request Form to the Information Officer. Please be aware that you may be required to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

## THE RIGHT TO OBJECT TO PROCESSING OF INFORMATION

You have the right, on reasonable grounds, to object to the processing of your personal information. In such circumstances, the Group will give due consideration to the request and the requirements of POPIA. The Group may cease to process your personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information. It should be noted that, if you object to the processing of your personal information, the Group will be unable to provide you with access to our services and products.

## CLIENT ACKNOWLEDGEMENT

I, \_\_\_\_\_, hereby acknowledge receipt of this POPIA Notice and Consent Form and confirm having read and understood the terms contained therein.

**Client Signature**

**Date**





# EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE



**HARVARD  
HOUSE**

We understand your need for  
FINANCIAL INTEGRITY

## DECLARATION

- “Personal Information” (PI) means the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the 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; the 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 views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- “POPIA” shall mean the Protection of Personal Information Act of 2013.
- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer’s relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by law.
- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore agrees:
  - That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer’s discharge of its obligations and to perform its functions as an employer.
  - That he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee’s PI by the employer for the purposes of securing and further facilitating the employee’s employment with the employer.
- Without derogating from the generality of the aforesaid, the employee consents to the employer’s collection and processing of PI pursuant to any of the employer’s Internet, Email and Interception policies in place insofar as the PI of the employee is contained in relevant electronic communications:
  - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee’s employment with the employer.
  - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee’s consent or to notify the employee of the reason for the processing of any of the employee’s PI.
  - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
  - To the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
  - To the employer transferring his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.
- The employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat such personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.

### The Harvard House Group:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd \*\*
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust \*\*
- Harvard House Insurance Brokers (Pty) Ltd \*\*

\*\* Authorised Financial Service Provider

- To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agrees to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.
- Employees may not directly or indirectly use, disclose or make public to any person or third party, either within the Group 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 on behalf of the employer.



# SLA CONFIDENTIALITY CLAUSE



**HARVARD  
HOUSE**

We understand your need for  
FINANCIAL INTEGRITY

## DECLARATION

- “Personal Information” (PI) means the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the 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; the 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 views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- “POPIA” means the Protection of Personal Information Act of 2013.
- The parties acknowledge that, for the purposes of this Agreement, they may come into contact with, or have access to, PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this Agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA’s Regulations and Codes of Conduct and that they shall only collect, use and process PI they come into contact with pursuant to this Agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this Agreement.
- The parties agree that they shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that they, or their employees, contractors or other authorised individuals come into contact with pursuant to this Agreement.
- Unless so required by law, the parties agree that they shall not disclose any PI, as defined in POPIA, to any third party without the prior written consent of the other party, and, notwithstanding anything to the contrary contained herein, they shall not transfer any PI out of South Africa.

### The Harvard House Group:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd \*\*
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust \*\*
- Harvard House Insurance Brokers (Pty) Ltd \*\*

\*\* Authorised Financial Service Provider

# INFORMATION OFFICER APPOINTMENT LETTER



**HARVARD  
HOUSE**

We understand your need for  
FINANCIAL INTEGRITY

## APPOINTMENT

You are hereby appointed as the Information Officer as required by the Protection of Personal Information Act of 2013 (POPIA). For the Harvard House Group, this appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the Group's reasonable compliance with the provisions of POPIA.
- Keeping the board of directors updated about the Group's information protection responsibilities under POPIA. In the case of a security breach, the Information Officer must inform and advise the board of directors of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the Group's personal information processing procedures. This will include reviewing the Group's information protection procedures and related policies.
- Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
- Ensuring that the Group makes it convenient for data subjects, who want to update their personal information or submit POPIA related complaints to the Group, to do so. For instance, maintaining a "contact us" facility on the Group's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the Group. This will include overseeing the amendment of the Group's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the Group are fully aware of the risks associated with the processing of personal information and that they remain informed about the Group's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the Group.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the Group's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The 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.

### The Harvard House Group:

- Harvard House Group Management Trust
- Harvard House Investment Management (Pty) Ltd \*\*
- Harvard House Chartered Accountants
- Harvard House Financial Services Trust \*\*
- Harvard House Insurance Brokers (Pty) Ltd \*\*

\*\* Authorised Financial Service Provider

## ACCEPTANCE

I hereby accept the appointment as Information Officer:

**Signature**

**Full Name**

**Date**

