

# POPIA and PAIA POLICY & MANUAL

In terms of Section 51 of POPIA No 4 of 2013

This Policy applies to **Smart Brats Nursery School**

Registration Number 1997/021121/23

(the "Company")

(Including all Subsidiaries)

01 June 2021

**Registered office address:**

1065 Koshuis Street  
Allens Nek  
1709

**Contact Details:**

**Telephone: 010 210 7150**

**Email: [info@smartbrats.co.za](mailto:info@smartbrats.co.za)**

THIS POLICY WAS PREPARED IN ACCORDANCE WITH THE  
POPIA NO 4 OF 2013 AND THE PAIA NO 2 OF 2000

## Contents

1.	DEFINITIONS .....	3
2.	INTRODUCTION .....	4
3.	DETAILS OF INFORMATION OFFICER.....	6
4.	THE ACT .....	7
5.	CODE OF CONDUCT .....	7
6.	POLICY WITH REGARD TO CONFIDENTIALITY AND ACCESS TO INFORMATION.....	7
7.	RECORDS AUTOMATICALLY AVAILABLE .....	8
8.	RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION:.....	8
9.	PARTICULARS IN TERMS OF SECTION 51 OF THE PAIA .....	9
10.	GUIDE ON HOW TO USE THE PAIA.....	9
11.	SUBJECTS AND CATEGORIES OF RECORDS HELD BY THE COMPANY .....	10
12.	RECORDS THAT ARE NOT AUTOMATICALLY AVAILABLE .....	11
13.	REQUEST PROCEDURE .....	11
14.	FEES.....	13
15.	THIRD PARTIES.....	14
16.	GROUNDS FOR REFUSAL OF ACCESS TO RECORDS // S62-69 OF THE ACT .....	14
18.	APPEAL - REMEDIES .....	15
19.	PROHIBITIONS OF SPECIAL PERSONAL INFORMATION .....	16
20.	DESTRUCTION OF INFORMATION.....	16

1. **DEFINITIONS**

“**Code of Conduct**” refers to a code of conduct issued under Chapter 7 of the Act;

“**Consent**” refers to any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of information;

“**Data Subject**” refer to a person to whom personal information relates;

“**De-identify**” refers to personal information of a data subject, means to delete information that-

- (a) identifies the data subject;
- (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; and
- (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

“**Filing System**” refers to any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

“**Information Officer**” refers the head of a private body as contemplated in Sect 1 of the PAIA;

“**Operator**” refers to a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party;

“**Person**” refers to a natural person or a juristic person;

“**Personal Information**” refers to information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including but not limited to –

- (a) Info relating to race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- (b) Info relating to education or medical, financial, criminal or employment history of a person;
- (c) Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to a person;
- (d) Biometric information of a person;
- (e) Personal opinion, views or preferences of a person;
- (f) Views of another person about a person

“**Processing**” refers to any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

- (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

- (b) dissemination by means of transmission, distribution or making available in any other form; or
- (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

“**Record**” refers to recorded information regardless of the form or medium, including written material, information produced (software) or devices or stored information;

## 2. INTRODUCTION

The **Promotion of Access to Information Act, 2000** (the “PAIA Act”) provides 3rd parties the right to approach private bodies and the government to request information held by them, which is required in the exercise and/or protection of any rights.

The **Protection of Personal Information Act, 2013** (the “POPI Act”) provides for the lawful procession of Personal Information by or for a responsible party as follow:

### 2.1. Accountability

The responsible party must ensure that conditions for lawful processing is implemented and controlled in terms of the purpose of such information and appointed accountability.

### 2.2. Processing Limitations

Personal Information must be processed in a lawful manner and in a reasonable manner that does not infringe on the privacy of the data subject.

Such processing of information may only be done if given the purpose for which it is intended to be processed, it is adequate, relevant and not excessive.

Processing of information may only be done where such processing is required for:

- 2.2.1. contractual obligations;
- 2.2.2. out of actions for conclusion or performance of a contract term to which the data subject is party to;
- 2.2.3. respective law / legislation;
- 2.2.4. protects the legitimate interest of the data subject;
- 2.2.5. necessary for the proper performance of a public law duty by a public body; and
- 2.2.6. pursuing the legitimate interest of a responsible party or 3<sup>rd</sup> party to whom the information is supplied.

Personal Information may only be collected directly from the data subject unless so derived from a public record or deliberately made public by the data subject.

### 2.3. Purpose specification

The Company must ensure that explicit reasoning and amendment of all source documentation is implemented in order to obtain the required permissions from all data subjects in terms of collection, processing and record keeping purposes.

Data retention may not exceed the legislative indications such as Financial Information, 10 years and Personnel Information 5 years.

Such permissions to retain information as per legislation or longer, must be in writing and explicitly agreed to by the data subject.

Destroying of information must be done in a controlled manner as to ensure that such destruction is legal and fully compliant with the knowledge of the data subject.

#### **2.4. Information Quality**

A reasonable person must take reasonable steps to ensure that information is accurate, up to date, not misleading or false, and completed.

#### **2.5. Openness**

The company must ensure that the data subject is well aware of the following:

- 2.5.1. What information is being collected, for what reason and where such information will be stored or processed;
- 2.5.2. Name and address of responsible person;
- 2.5.3. Purpose of collection;
- 2.5.4. Mandatory and voluntary information collection;
- 2.5.5. Consequences for failing to provide correct and accurate information;
- 2.5.6. What transfer is intended to be transferred or utilized in terms of contractual obligations and with which 3<sup>rd</sup> party;
- 2.5.7. Any objection by the data subject submission in storing or processing of any information.

#### **2.6. Security safeguard**

The Company must ensure that the integrity and confidentiality of all data subject information in its possession or under its control is maintained at all times by taking appropriate, reasonable, technical and organisational measures to prevent loss, damage or unlawful usage of such information.

The company must ensure that a comprehensive agreement between consultants and / or service providers entrusted with such processing of personal information is undersigned with limitations and restrictions as per the Act on such Businesses.

Regular audits and confirmations are to be implemented to ensure full compliance on an annual basis.

#### **2.7. Data subject participation**

A data subject, where adequate proof of identification has been provided, may request a responsible party to confirm whether or not a reasonable party holds personal information about the data subject. Any such records may be requested with instruction to destroy and / or maintain control over such information.

Where such information or confirmation of stored information is requested, the responsible party / person / company will have 30 days to confirm and / or supply such information.

## POPIA & PAIA POLICY

A data subject may be requested to confirm current and / or active information with the responsible person annually and / or request to have amendments / changes made to such information in order to update and / or amend information from time to time.

**Constitution of the Republic of South Africa, 1996** section 14, provides that everyone has the right to privacy. The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

The POPI Act gives a Data Subjects the right to, in the prescribed manner, request a Responsible Party to correct, amend, change or delete Personal Information about the Data Subject in its possession or under its management and control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. Such information may be requested to be destroyed or to delete a record of Personal Information about the Data Subject that the Responsible Party is no longer authorised to retain access and/or request the correction or deletion of any Personal Information held about them that may be inaccurate, misleading or outdated.

The Company endorses and complies with the PAIA Act and POPI Act and believes that this Policy will assist all in exercising their rights and obligations. The Act seeks, *inter alia*, to give effect to the constitutional right of access to any information held by the state or by any other person where such information is required for the exercise or protection of any right.

### 3. DETAILS OF INFORMATION OFFICER

The Information Officer of the Company is referred to as the head of a private body or an identified or appointment Information Officer who is responsible for and accountable for all matters pertaining to the Acts and this Policy.

The Company hereto note that the following identified, trained and orientated individual are appointed in terms of the Information Officer:

Name:	Nicola Hultum
Physical Address:	1065 Koshuis Street
	Allens Nek
	1733
	Johannesburg
	Republic of South Africa

Telephone Number: 010 210 7150

E-mail: [info@smartbrats.co.za](mailto:info@smartbrats.co.za)

#### 3.1. Duties and Responsibilities of an Information Officer

The appointment of an Information Officer is made by the Company Shareholders / Management and / or Owner in terms of the law. Where so deemed necessary a Deputy Information Officer may be appointed at the discretion of the Company.

The responsibilities include:

- ✓ Encouraging of compliance amongst staff and responsible departments;
- ✓ Managing requests made by data subjects (external and internal);
- ✓ Co-operating with the Regulator in terms of audits, compliance audits and respective measures;

#### **4. THE ACT**

The ACT grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

Requests in terms of the ACT shall be made in accordance with the prescribed procedures, at the rates provided.

Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission, which will contain information for the purposes of exercising Constitutional Rights. The Guide is available from the SAHRC.

#### **5. SCOPE**

This Policy has been prepared in respect of the Company or Group of Companies, which includes the following related entities:

- ✓ Smart Brats Nursery School

The scope of this Policy excludes the Company's operations outside the Republic of South Africa and will serve to provide a reference regarding the records held by the Company at its Registered Office and various operations within the borders of the Republic of South Africa.

#### **6. CODE OF CONDUCT**

It is advisable that every person responsible for maintaining control and safeguarding, processing and managing of personal information be issued with a code of conduct that is required to be undersigned and duly followed, in terms of the following:

- 6.1. Conditions under which the lawful processing of personal information may be conducted;
- 6.2. Conditions setting out the functional equivalent of all the obligations of such conditions;
- 6.3. Description of how lawful actions must be conducted;
- 6.4. Specify measures to be taken in storing data, disposing of data, manage requested data, legislative indications on data, etc.

The Company is required to set up complaint channels and procedures in terms of this Policy. Clear terms and timelines must be communicated in terms of managing complaints with record keeping.

#### **7. POLICY WITH REGARD TO CONFIDENTIALITY AND ACCESS TO INFORMATION**

The Company will protect the confidentiality of information provided to it by a data subject or 3rd parties, subject to the Company's obligations to disclose information in terms of any

applicable law or regulation or a court order requiring disclosure of information. If access is requested to a record that contains information about a 3rd party, the Company is obliged to attempt to contact such 3rd party or data subject to inform them of the request.

The Company will give the party an opportunity of responding by either consenting to the access or by providing reasons why the access should be denied. In the event that the party furnishing reasons for the support or denial of access, the Information Officer will consider these reasons in determining whether access should be granted to the requestor or not.

**8. RECORDS AUTOMATICALLY AVAILABLE**

The categories of records that are automatically available without a person having to request access in terms of the PAIA Act [Section 51(1)(c)].

- ✓ Records of the Company lodged in terms of government requirements such as the Registrar of Deeds;
- ✓ Documentation and information relating to the Company which is held by the Companies and Intellectual Properties Commission in accordance with the requirements set out in set out in section 25 of the Companies Act 71 of 2008;
- ✓ Product and Services Brochures; and
- ✓ News and other Marketing Information.

Certain other information relating to the Company’s is also made available on said website from time to time, which is deemed public record.

**9. RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION:**

Records are kept in accordance with such other legislation as applicable to the Company, which includes, but is not limited to:

<u>No</u>	<u>Reference</u>	<u>Act</u>
1	No 61 of 1973	Companies Act
2	No 98 of 1978	Copyright Act
3	No 55 of 1998	Employment Equity Act
4	No 95 of 1967	Income Tax Act
5	No 66 of 1995	Labour Relations Act
6	No 89 of 1991	Value Added Tax Act
7	No 37 of 2002	Financial Advisory and Intermediary Services Act
8	No 75 of 1997	Basic Conditions of Employment Act
9	No 69 of 1984	Close Corporations Act
10	No 25 of 2002	Electronic Communications and Transactions Act
11	No 02 of 2000	Promotion of Access of Information Act
12	No 30 of 1996	Unemployment Insurance Act

## **10. PARTICULARS IN TERMS OF SECTION 51 OF THE PAIA**

- 10.1. The PAIA Act seeks to advance a culture of transparency and accountability in both public and private bodies. The legislation was enacted as a direct response to Section 32(2) of the Constitution of South Africa (the right of access to information) which requires that the Government implements laws in an effort to make information pertaining to public and private bodies more accessible to all.
- 10.2. The Act gives effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights. Where a request is made in terms of the PAIA Act, the body to whom the request is made is obliged to release the information, except where the PAIA Act expressly provides that the information may or must not be released.
- 10.3. One of the main requirements specified in the PAIA Act is the compilation of a Policy that provides information on both the types and categories of records held by the public or private body. In terms of the PAIA Act, the Company is regarded as a “private body” and therefore the requirements regarding access must follow the provisions of the PAIA Act relevant to private bodies and more in particular Section 51 of the PAIA Act.
- 10.4. In compliance with Section 51 of the PAIA Act this PAIA Policy sets out the following details:
  - 10.4.1. The Company’s contact details including, physical and postal addresses, telephone and fax numbers, electronic mail address of the person tasked in terms of this Code of Conduct;
  - 10.4.2. Information on how to obtain and access this Code of Conduct and a guide on how to use it;
  - 10.4.3. Categories of information held by the Company that is available without a person having to formally request such details in terms of the PAIA Act;
  - 10.4.4. Categories of information held by the Company that is available in accordance with other legislation and which, subject to the PAIA Act, may be made available by the Company on receipt of and consideration of a formal request, made in terms of the PAIA Act;
  - 10.4.5. Sufficient information to facilitate a request for access to records and a description of the subjects on which records are available from the Company;
- 10.5. Adherence to these requirements entails not only compilation of the external Policy but also compliance with the general provisions stated in the PAIA Act.

## **11. GUIDE ON HOW TO USE THE PAIA**

- 11.1. The Human Rights Commission has been tasked with the administration of the PAIA Act.
- 11.2. In terms of Section 10 of the PAIA Act, the Human Rights Commission has compiled a guide which is intended to assist users in the interpretation of the PAIA Act and how to

access the records of private and public bodies and the remedies available in law regarding a breach of any of the provisions of the PAIA Act.

- 11.3. Should any person have queries or concerns relating to their rights and in particular their right to access information from a private or public body, such queries should be directed to:

The South African Human Rights Commission PAIA Unit  
Private Bag X2700  
Houghton, 2041  
Republic of South Africa

Business phone: +27 11 877 3600  
Fax: +27 11 403 0625  
Email address: [section51.paia@sahrc.org.za](mailto:section51.paia@sahrc.org.za)  
Website: [www.sahrc.org.za](http://www.sahrc.org.za)

## 12. SUBJECTS AND CATEGORIES OF RECORDS HELD BY THE COMPANY

The list below depicts records of information which the Company has available in terms of laws applicable to the Company:

### 12.1. Corporate Secretariat and Governance

- ✓ Applicable Statutory Documents
- ✓ Policies and Procedures
- ✓ Code of Conduct
- ✓ Records relating to the appointment of directors and auditor
- ✓ Health & Safety Records
- ✓ Share Certificates
- ✓ Legal Compliance Records
- ✓ Share Register and other statutory registers
- ✓ Memoranda of Incorporation
- ✓ Statutory Returns to Relevant Authorities

### 12.2. Finance and Taxation

- ✓ Accounting Records (including Ledgers and Reconciliations)
- ✓ Annual Financial Statements
- ✓ Audit Report (where applicable)
- ✓ Client information in terms of a Service Level Agreement
- ✓ Bank Records and Statements
- ✓ SARS records (PAYE, UIF and SDL)
- ✓ SARS records of employees (IRP5's)
- ✓ Debtors and Creditors statements and invoices
- ✓ Income Tax numbers of Staff
- ✓ VAT numbers of clients
- ✓ Workmen's Compensation Returns and LOGS

**12.3. Personal Documents and Records**

- ✓ CV's, application forms and personal details of any applicant
- ✓ Personal information including ID's, Criminal Checks, References, Banking details
- ✓ Disciplinary Code and Records
- ✓ Leave Records
- ✓ Job Profiles
- ✓ Letters of Appointment and Contracts
- ✓ Dispute resolution records
- ✓ Organisational Structures
- ✓ Employment Equity information
- ✓ Termination Documentation
- ✓ Qualifications
- ✓ Payroll reports and information
- ✓ Employee Benefit forms and information (3<sup>rd</sup> party requirements)

**12.4. Intellectual Property**

- ✓ Intellectual property pertaining to solutions and
- ✓ Know-how products developed

**12.5. Corporate Affairs and Investor Relations / Communications**

- ✓ Media Releases
- ✓ Newsletters and Publications

**12.6. Legal**

- ✓ Agreements and Contracts
- ✓ Health and Safety Records
- ✓ Client disputes and client employee disputes

**12.7. Sales, Marketing and Communications**

1. Actual Sales
2. Branding
3. Press releases / communique
4. External Publications
5. Media and advertising
6. Proposals and Tenders

**13. RECORDS THAT ARE NOT AUTOMATICALLY AVAILABLE**

Records of the Company which are not automatically available must be requested in terms of the procedure set out in this Policy and which may be subject to the restrictions and right of refusal to access as provided for in the Act.

**14. REQUEST PROCEDURE**

- 14.1. The Company is mainly concerned about protecting the confidential information of its Data Subjects at all times.

## POPIA & PAIA POLICY

- 14.2. Any person making a request for access to records of the Company is referred to as a “requester”. The requester must comply with all the procedural requirements contained in the PAIA Act relating to the request for access to records.
- 14.3. The requester must complete the prescribed form application form attached hereto as **Form C** and submit the form, to the Information Officer of the Company at the postal or physical, fax or electronic mail address as stated above.
- 14.4. The prescribed form must be filled in with sufficient particulars to at least enable the Information Officer of the Company to identify:
  - 14.4.1. record or records requested;
  - 14.4.2. identity of the requester;
  - 14.4.3. which form of access is required if the request is granted; and
  - 14.4.4. postal address, telephone number and fax number of the requester.
- 14.5. The requester must state that he/she requires the information to exercise or protect her/his right and clearly state what the nature of the right is to be exercised or protected. In addition, the requester must clearly specify why the records are necessary to exercise or protect such a right.
- 14.6. Such request must be processed within 30 (thirty) days after the request has been received.
- 14.7. The requester shall be informed whether the access has been granted or denied within 30 (thirty) days of receipt of the request and give notice with reasons to that effect.
- 14.8. The 30 (thirty) day period within which the Company must decide whether to grant or refuse the request, may be extended for a further period of not more than 30 (thirty) days if the request is for a vast amount of information, or the information cannot reasonably be obtained within the original 30 (thirty) day period. The Information Officer will notify the requester in writing should an extension be sought.
- 14.9. If the request for access is granted, the Deputy Information Officer of the Company must advise the requestor:
  - 14.9.1. the access fee (if any) to be paid upon access;
  - 14.9.2. the form in which access will be given; and
  - 14.9.3. that the requester may lodge an application with a court against the access fee to be paid or the form of access granted, and the procedure, including the period allowed, for lodging the application.
- 14.10. If the request for access is refused, the Information Officer of the Company must:
  - 14.10.1. state adequate reasons for the refusal, including the provisions of this Act relied on;
  - 14.10.2. exclude, from any such reasons, any reference to the content of the record; and

- 14.10.3. state that the requester may lodge an application with a court against the refusal of the request, and the procedure (including the period) for lodging the application.
- 14.11. In terms of Section 54 of the PAIA Act, if all reasonable steps have been taken to find the record requested and there are reasonable grounds to believe that the record is in possession of the Company but cannot be found, and if it does not exist, then the Information Officer of the Company must notify by way of affidavit or affirmation, the requester that it is not possible to give access to that record.
- 14.12. If after notice is given, the record in question is found, the requester must be given access thereto unless the ground for the refusal of access exists.
- 14.13. If the request is declined for any reason the notice must include adequate reasons for the decision, together with the relevant provisions of the PAIA Act relied upon and provide the procedure to be followed should the requester wish appeal the decision.
- 14.14. Section 59 provides that the Information Officer of the Company may serve a record and grant access only to that portion which the law does not prohibit access to.

## **15. FEES**

- 15.1. The Act provides for two types of fees, namely:
  - 15.1.1. A request fee, which will be a standard fee; and
  - 15.1.2. An access fee, which must be calculated by considering reproduction costs, search and preparation time and costs, as well as postal costs.
- 15.2. When the request is received by the Information Officer of the Company, such person shall by notice require the requester to pay the prescribed request fee, if any, before further processing of the request.
- 15.3. If a requester requires access to records of his/her Personal Information, there shall be no request fee payable. However, the requester must pay the prescribed access and reproduction fees for such Personal Information.
- 15.4. If the search for the record has been made and the preparation of the record for disclosure including arrangements to make it available in the request form, requires more than the hours prescribed in the regulations for this purpose, the Deputy Information Officer of the Company shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.
- 15.5. The Information Officer of the Company shall withhold the record until the requester has paid the fees as indicated hereto.
- 15.6. A requester whose request for access to a record has been granted, must pay an access fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the records for disclosure including making arrangements to make it available in the request form.

- 15.7. If a deposit has been paid in respect of a request for access, which is refused, then the Deputy Information Officer of the Company must repay the deposit to the requester with interest at the prescribed rate.

## 16. THIRD PARTIES

- 16.1. If the request is for the record pertaining to the third party, the Information Officer of the Company must take all reasonable steps to inform the third party of the request. This must be done within 21 (twenty-one) days of receipt of the request. The way this is done must be by the fastest means reasonably possible, but if orally, the Information Officer of the Company must thereafter give the third party a written confirmation of the notification.
- 16.2. The third party may within 21 (twenty-one) days thereafter either make representation to the Company as to why the request should be refused; alternatively grant written consent to the disclosure of the record.
- 16.3. The third party must be advised of the decision taken by the Information Officer of the Company whether to grant or to decline the request. A third party who is dissatisfied with the Information Officer of the Company's decision to grant a request for information, may within 30 (thirty) days of notification of the decision, apply to a Court for relief.

## 17. GROUNDS FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF SECTION 62-69 OF THE ACT

The Company has the right to refuse access to information on one or more of the following grounds:

- 17.1. ***Mandatory protection of the privacy of a third party who is a natural person***, if such disclosure would involve the unreasonable disclosure of Personal Information about a third party, including a deceased individual, subject to the provisions of section 63 (2).
- 17.2. ***Mandatory protection of the commercial information of a third party***, if the record contains:
- 17.2.1. Trade secrets of that party;
  - 17.2.2. Financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interest of that third party;
  - 17.2.3. Information disclosed in confidence by a third party, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition;
  - 17.2.4. Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.
- 17.3. ***Mandatory protection of certain confidential information of third party***, where the head of a private body must refuse a request for access to a record of the body if its

disclosure would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement.

- 17.4. **Mandatory protection of the safety of individuals and the protection of property**, where such disclosure could endanger the life or physical safety of an individual, or prejudice or impair the security of:

- 17.4.1. a building, structure, or any system
- 17.4.2. a means of transport, or
- 17.4.3. any other property.

- 17.5. **Mandatory protection of records, which would be regarded as privileged from production in legal proceedings.**

- 17.6. **Commercial information of private body**, in that a request for access to a record may be refused if the record contains:

- 17.6.1. trade secrets, financial, commercial, scientific, or technical information of the institution, which disclosure, could likely cause harm to the financial or commercial interest of the institution;
- 17.6.2. Information which, if disclosed could prejudice or put the institution at a disadvantage in negotiations or commercial competition; and
- 17.6.3. A computer program which is owned by the institution and which is protected by copyright.

- 17.7. **Mandatory protection of research information of the institution.** A request will be refused if this disclosure would disclose the identity of the institution, the researcher or the subject matter of the research and would place the researcher at a serious disadvantage.

- 17.8. **Mandatory disclosure in public interest.** Despite any of the protections mentioned above, the Director of the Company shall grant a request for access to a record if:

- 17.8.1. the disclosure of the record would reveal evidence of-
  - 17.8.1.1. a substantial contravention of, or failure to comply with, the law; or
  - 17.8.1.2. imminent and serious public safety or environmental risk; and
- 17.8.2. the public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question.

## 18. APPEAL - REMEDIES

- 18.1. The Company does not have an internal appeal procedure. As such, the decision made by the Information Officer of the Company is final and requesters will have to exercise such external remedies at their disposal if the request for information is refused and the requester is not satisfied with the answer supplied by the Information Officer of the Company.

- 18.2. If a requester is aggrieved by the refusal of the Information Officer to grant a request for a record, the requester may, within thirty (30) days of notification of the Information Officer's decision, apply to court for appropriate relief.
- 18.3. The court will review the request and decide whether in fact the Information Officer of the Company should give the requester the information requested or not. A court hearing an application in terms of the PAIA Act may grant any order that is just and equitable including orders:
  - 18.3.1. confirming, amending, or setting aside the decision which is the subject of the application;
  - 18.3.2. requiring the Deputy Information Officer of the Company or relevant authority of a public body or the head of a private body to take such action or to refrain from taking such action, as the court considers necessary within the period mentioned in the court order;
  - 18.3.3. granting an interdict, interim or specific relief, a declaratory order or compensation; or
  - 18.3.4. granting an order as to costs.

## **19. PROHIBITIONS OF SPECIAL PERSONAL INFORMATION**

A responsible party may not process personal information concerning:

- 19.1. Religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
- 19.2. The criminal behaviour of a data subject to the extent that such information relates to the alleged commission by the data subject of any offence and any proceedings in respect of the offence allegedly committed.

Unless such information forms part of public interest or record or deemed required by a Court of Law.

A data subject can provide written permission for the responsible person to declare or make public such information.

Information must be processed and supplied in all cases as mentioned hereto where such information forms part of a legislative requirement and / or in the interest of the party required, such as Trade Union information, registered institutions, etc.

## **20. DESTRUCTION OF INFORMATION**

- 20.1. Information destruction must be reviewed at the level of requirements as set out by POPIA as well as the security safeguards of such information.
- 20.2. It is not sufficient to destroy or shred information internally that is deemed or classified under level 2 as per below. It is recorded that the Company will be deemed non-compliant where such structures are not correctly followed:

20.2.1. **Protection class 1**

- Normal security for internal data (such as paper with no confidential information, printing plates, etc.)
- **Security level: DIN P-1, DIN P-2, DIN P-3**
- Classification Level 1 being protected by Security Level 1 or 2 methods – in other words a traditional ribbon or strip cut shredding process is inadequate for POPI Act needs

20.2.2. **Protection class 2**

- High security for confidential data such as “Unauthorised disclosure would have serious effects” and “may lead to violations of laws or contractual obligations”. At Classification Level 2 protection of personal data will meet “stringent requirements”.
- **Security level: DIN P-3, DIN P-4, DIN P-5**

20.2.3. **Protection class 3**

- Very high protection for confidential and secret data addresses confidential and secret information where unauthorised disclosure would have “serious existence-threatening effects” and protection of personal data will be absolutely guaranteed.
- Security Levels 4 to 7 should be used for the highest Classification Level 3 information destruction
- **Security level: DIN P-4, DIN P-5, DIN P-6, DIN P-7**

20.3. The POPIA requires a business to use a Cross-Cut Shredder, (P-3 or P-4) or a Micro-Cut Shredder (P-5) and to be really safe, use a Super Micro-Cut Shredder (P-6) or a Super Fine Micro-Cut Shredder (P-6+).

Duly so undersigned and implemented at \_\_\_\_\_ on this \_\_\_\_\_ day of June 2021

---

XX

OWNER / DIRECTOR

**FEES IN TERMS OF PAIA**

**NOTICE IN TERMS OF THE PROMOTION OF ACCESS TO INFORMATION 2 OF 2000  
RE: FEES ASSOCIATED WITH PAIA REQUESTS ARE DETERMINED BY THE  
REGULATIONS ONLY AND NOT THROUGH OTHER APPLICABLE LAWS OR POLICIES**

This Notice serves to state that the South African Human Rights Commission (the Commission) hereby confirms that the costs associated with all requests made under the Promotion of Access to Information Act 2 of 2000 (PAIA) are determined by the Regulations relating to PAIA only, and not by any other laws or regulations. Therefore, any demands made by a public or private body for the payment of additional fees with respect to PAIA requests are invalid.

The Commission is an independent public body currently mandated under PAIA to monitor the implementation of the Act. In accordance with its responsibilities to ensure compliance with PAIA, the Commission issues this notice to bring clarity to all interested parties that it is *only* the Minister of Justice and Constitutional Development who has the power to make decisions regarding fees associated with PAIA requests. The Commission further confirms that Value-Added Tax (VAT) is only payable by institutions who have registered as VAT vendors.

**1. The Promotion of Access to Information Act**

PAIA gives effect to the constitutional right to access of information, as provided for under section 32 of the Constitution. Although responding to requests and reproducing records in an accurate and orderly manner takes time and resources, section 9 of the Act specifically calls for the establishment of mandatory mechanisms and procedures to ensure that access to records of both public and private bodies is "as swiftly, *inexpensively* and effortlessly as reasonably possible." [emphasis added].

Furthermore, section 92 of the Act grants the Minister of Justice and Constitutional Development the power to make regulations pertaining to fees associated with requests made to both public and private bodies.

**2. Regulations to PAIA**

In February 2002, the Minister of Justice and Constitutional Development published a schedule of fees for PAIA requests in the Gazette, which provided for the following:

Fees for Requesting Records

Requesters are required to pay a fee for requesting access to records from both public and private bodies. The fee for requesting records from a public body is R35, while the fee for requesting records from a private body is R50. It is important to note that people who are requesting access to their personal information are exempt from paying a fee. Furthermore, people who earn less than R14,712 per annum (if single) and R27,192 per annum (if married or have a life partner), are also exempt from paying the request fees.

Fees for Accessing Records

Requesters are also required to pay fees for accessing the records of public and private bodies, which include fees associated with the search for, preparation of, and reproduction of documents. The breakdown of fees for requests to both public and private bodies are as follows:

**Public Bodies:**

- Copy per A4 page – 60 cents
- Printing per A4 page – 40 cents
- Copy on a CD – R40
- Transcription of visual images per A4 page – R22
- Copy of a visual image – R60
- Transcription of an audio recording per A4 page – R12
- Copy of an audio recording – R17
- Search and preparation of the record for disclosure – R15 per hour or part thereof, excluding the first hour, reasonably required for the search and preparation
- Actual postage fee

**Private Bodies:**

- Copy per A4 page – R1.10
- Printing per A4 page – 75 cents
- Copy on a CD – R70
- Transcription of visual images per A4 page – R40
- Copy of a visual image – R60
- Transcription of an audio recording per A4 page – R20
- Copy of an audio recording – R30
- Search and preparation of the record for disclosure – R30 per hour or part thereof, excluding the first hour, reasonably required for the search and preparation
- Actual postage fee

**3. Registered VAT Vendors**

The Commission further confirms that Value-Added Tax (VAT) is only payable by institutions who have registered as VAT vendors, as required under section 23 of the Value-Added Tax Act of 1991.

Sincerely,



Advocate L M Mushwana

Chair of the South African Human Rights Commission

**COMPLIANCE INDICATOR**

Every Business must ensure that a Policy / Manual is present within the Business. Declarations and submission of Businesses are guided below.

Submissions must be made on or by **30 April** of every year.

<b>Industry or sector</b>	<b>Turnover Threshold</b>
Agriculture	R6 million
Mining and Quarrying	R22,5 million
Manufacturing	R30 million
Electricity, Gas and Water	R30 million
Construction	R15 million
Retail and Motor Trade and Repair Services	R45 million
Wholesale Trade, Commercial Agents and Allied Services	R75 million
Catering, Accommodation and other Trade	R15 million
Transport Storage and Communications	R30 million
Finance and Business Services	R30 million
Community, Special and Personal Services	R15 million