

Title: PAIA and POPIA Policy Manual

Unique Identifier: QMP 6.2.12

Valid as of: 1 July 2021

Revision: Rev. 1

Revision date: 24.10.23

Total Pages: 29

Compiled By:

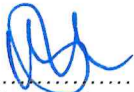
Functional Responsibility:

Authorized By:

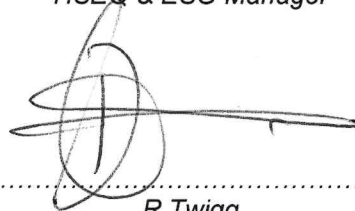
QA Manager

HSEQ & ESG Manager

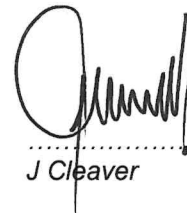
Managing Director




.....
R Mulaudzi



.....
R Twigg



.....
J Cleaver


PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 2 of 29	

CONTENTS

1	Introduction	3
2	Objective	3
3	Scope	3
4	Definitions	3
5	References	4
6	Appointment of Information Officer and Deputy Information Officer	5
7	Guide to SA Human Rights Commission	6
8	Access to Information Available Only on Request	6
9	Records Available Without a Request to Access	8
10	Description of Information which are Available in Terms of Any Other Legislation	8
11	Detail to Facilitate a Request for Access to a Record of KAEFER	9
12	Refusal of Access to Records	10
13	Remedies Available When KAEFER Refuses Request	11
14	Access to Records Held by KAEFER	11
15	Prescribed Fees for Access to Information	12
16	Decision	12
17	Protection of Personal Information that is Processed by KAEFER	12
17.1	Data Subjects Rights	13
17.2	Personal Information that KAEFER Collects	13
17.3	Purpose of Processing Personal Information	13
17.4	Recipients of Personal Information	13
17.5	Cross-border Flows of Personal Information	13
17.6	Obtaining Written Consent	14
17.7	Objection to the Processing of Personal Information	17
17.8	Request for Correction or Deletion of Personal Information	17
18	Automated Decision Making	17
19	Procedure for Processing of Personal Information by KAEFER Employees and Other Persons Acting on Behalf of KAEFER	17
20	Information Security	19
21	Training	21
22	Data Breach Incident Report	21
23	Disciplinary Action	22
24	POPIA/PAIA Auditing	23
25	Legal Requirements	23
26	Management Review	23
27	Duties and Responsibilities	24
28	10 Practical Measures for Compliance	26
29	FAQ	27
30	Availability and Updating of Manual	29
31	Change Tracking History	29
31	Annexures	29

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 3 of 29	

1. INTRODUCTION

KAEFER collects and processes personal data relating to its employees, suppliers, and clients and is committed to meeting its data protection obligations.

This manual was prepared in accordance with section 51 of the Promotion of Access to Information Act, 2000 and to address requirements of the Protection of Personal Information Act, 2013.

2. OBJECTIVE

To identify the process to be followed across the lifecycle of the personal information, as well as, to strike a balance between the right to privacy and the need for the free flow of, and access to information.

3. SCOPE


This policy applies to all employees of KAEFER, including its affiliated companies, who access, process, or keep any type of records relating to the personal information of persons or entities.

This policy prescribes minimum requirements. Where there is conflict between this policy and regulatory or statutory requirement, the relevant applicable stricter requirement shall apply.

This policy shall be read and implemented in conjunction with the KAEFER Code of Business Conduct, QMP 5.3.1 and POPI Act Privacy Policy, KTQ 235.

4. DEFINITIONS

POPI/POPIA	Protection of Personal Information Act No.4 of 2013
PAIA	Promotion of Access to Information Act, 2000
Data Subject:	A person/entity to whom the personal information relates
Direct Marketing:	Sending a data subject an electronic communication about goods and services that you are promoting or offering to supply in the ordinary course of business or requesting a donation of any kind for any reason.
Processing:	Any operation or activity concerning personal information.
Record:	Any recorded information, regardless of when it came into existence.
Responsible Party:	A public or private body or any other person which determines the purpose of and means for processing personal information.

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi Approved By: J. Cleaver Date: 24/10/23	Serial No: QMP 6.2.12 Revision: 1 Page 4 of 29	

De-identify: means to delete any information that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject;

Information Regulator: Appointed by the President to implement the terms of and manage the POPI Act.

Personal Information: Information relating to an identifiable, living, natural person or an identifiable, existing juristic person. It ranges from information relating to race, gender, sex, pregnancy, marital status, ethnic or sexual orientation, age, physical or mental health, to the views or opinions of another individual.

Special Personal Information: This relates to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information

5. REFERENCES

Promotion of Access to Information Act, 2000 (POPIA)

Protection of Personal Information Act, 2013 (PAIA)

General Data Protection Regulations (EU) (GDPR)

ISO 27001

POPI Act Privacy Policy Statement KTQ 235

KAEFER Code of Conduct QMP 5.3.1

Disciplinary Procedure QMS 6.2.5

Internal Audit Procedure QMS 8.2.2

Preventive and Corrective Procedure QMS 8.5.2

Management Review Procedure QMS 5.6

IT Governance Rule QMP 5.3.1

6. APPOINTMENT OF INFORMATION OFFICER AND DEPUTY INFORMATION OFFICERS


The Information Officer is responsible for ensuring that the Company complies with the requirements of POPIA and PAIA. This position is automatically assigned to the Head of an Organisation, such as the CEO/MD.

Contact Details of the Managing Director - Section 51(1)(a)

MD	Jayson Cleaver
Registered Address:	7 Nywerheid Street, Tunney, Elandsfontein, Germiston
Postal Address:	P O Box 902, Isando, 1600
Telephone Number:	011 974 8123
Email Address:	jayson.cleaver@kaefer.co.za
Website:	www.kaefer.co.za

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 5 of 29	

At KAEFER, the MD has appointed an Information Officer, as allowed in terms of section 17 of PAIA as well as section 55 of the POPIA, to assist in his duties which are amongst other things:

- Ensuring that the organization complies with the conditions of lawful processing of personal information; and
- Working with the Regulator in relation to any investigations conducted in accordance with the relevant provisions of POPIA and PAIA

*See Section 25 for full duties.

The Appointed Information Officer for KAEFER is:

Information Officer:	Renata Twigg
Registered Address:	7 Nywerheid Street, Tunney, Elandsfontein, Germiston
Postal Address:	P O Box 902, Isando, 1600
Telephone Number:	011 974 8123
Email Address:	renata.twigg@kaefer.co.za
Website:	www.kaefer.co.za

Additionally, **two** Deputy Information Officers have been appointed to assist the Information Officer:

Deputy Information Officer:	Rathiaya Mulaudzi
Telephone Number:	011 974 8123
Email Address:	Rathiaya.mulaudzi@kaefer.co.za

Deputy Information Officer:	Muhuliseni Mathidi
Telephone Number:	011 974 8123
Email Address:	muhuliseni.Mathidi@kaefer.co.za

The Information Officer and all Deputy Information Officers must be registered with the Information Regulator.

7. GUIDE TO SA HUMAN RIGHTS COMMISSION (Section 51 (1)(b))

PAIA grants a requester access to records of a private body, if the record is required to exercise or for the 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 PAIA shall be made in accordance with the prescribed procedures.

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

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 6 of 29	

The contact details of the Commission are:

Contact Body:	The South African Human Rights Commission
Physical Address:	Braampark Forum 3, 33 Hoofd Street, Braamfontein, JOHANNESBURG
Postal Address:	Private Bag 2700, Houghton 2041
Telephone Number;	+27 11 877 3600
Email address:	info@sahrc.org.za
Website:	www.sahrc.org.za

8. ACCESS TO INFORMATION AVAILABLE ONLY ON REQUEST (Section 51 (1)(e))

8.1. Subjects and Categories of Records held by KAEFER


The Company collects and processes a range of information about its employees. This includes, without limitation, directors (executive and non-executive), all permanent, temporary, part-time staff, as well as Clients and any other person/entity who assists in carrying out or conducting the business of KAEFER.

The following schedule serves as a reference to the categories of information that KAEFER holds.

Subject	Category
Companies Act Records	Trust deeds. Documents of Incorporation. Index of names of Directors. Memorandum of Incorporation. Minutes of meetings of the Board of Directors. Minutes of meetings of Shareholders. Proxy forms. Register of directors' shareholdings. Share certificates. Share Register and other statutory registers and/or records and/or documents. Special resolutions/Resolutions passed at General and Class meetings; Records relating to the appointment of: Auditors, Directors, Prescribed Officer, Public Officer; and Secretary
Financial Records	Accounting Records. Annual Financial Reports. Annual Financial Statements Asset Registers. Bank Statements. Banking details and bank accounts. Banking Records. Debtors / Creditors statements and invoices.

CONTROLLED DISCLOSURE


When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 7 of 29	

Subject	Category
	General ledgers and subsidiary ledgers; General reconciliation. Invoices. Paid Cheques. Policies and procedures. Rental Agreements, and Tax returns
Income Tax Records	PAYE Records. Documents issued to employees for income tax purposes. Records of payments made to SARS on behalf of employees. All other statutory compliances: To VAT Regional Services Levies Skills Development Levies UIF or Workmen's Compensation
Personnel Documents and Records	Disciplinary Code and Records. Employee benefits arrangements rules and records. Employment Contracts. Employment Equity Plan Forms and Applications. Grievance Procedures. Leave Records. Medical Aid Records. Payroll reports/ Wage register. Pension Fund Records. Salary Records. SETA records Standard letters and notices Training Manuals. Training Records. Workplace and Union agreements and records. Next of kin and personal details
Procurement Department	Standard Terms and Conditions for supply of services and products. Contractor, Client and Supplier agreements. Lists of suppliers, products, services and distribution; and Policies and Procedures. Customer details Credit application information Information and records provided by a third party
Business Development/Estimating Department	Customer details Credit application information Information and records provided by a third party
Marketing Department	Advertising and promotional material
HSEQS & Security	Audit reports. Security entry registers COVID screening Risk management frameworks; and Risk management plans. Safety, Health and Environment Procedures Complete Safety, Health and Environment Risk Assessment

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi Approved By: J. Cleaver Date: 24/10/23	Serial No: QMP 6.2.12 Revision: 1 Page 8 of 29	

Subject	Category
	HSE Plans Inquiries, inspections, and investigations by DOL CSR/SED schedule of projects/record of organizations that receive funding. Reports, books, publications, and general information related to CSR/SED spend. Records and contracts of agreement with funded organizations
IT Department	Computer / mobile device usage policy documentation. Disaster recovery plans. Hardware asset registers. Information security policies/standards/procedures. Information technology systems and user manuals Information usage policy documentation. Project implementation plans. Software licensing; and System documentation and manuals.

Note that the accessibility of the records may be subject to the grounds of refusal, as set out in this manual. Amongst other, records deemed confidential on the part of a third party, will necessitate permission from the third party concerned, in addition to normal requirements, before KAEFER will consider access.

9. RECORDS AVAILABLE WITHOUT A REQUEST TO ACCESS

Records of a public nature, typically those disclosed on the KAEFER website, and other non-confidential records, such as statutory records maintained at CIPC, may be accessed without the need to submit a formal application.

10. DESCRIPTION OF INFORMATION WHICH ARE AVAILABLE IN TERMS OF ANY OTHER LEGISLATION (Section 51(1)(d))


Where applicable to its operations, KAEFER also retains records and documents in terms of the legislation listed below.

Unless disclosure is prohibited in terms of legislation, regulations, contractual agreement or otherwise, records that are required to be made available in terms of the following Acts, shall be made available for inspection by interested parties.

- Auditing Professions Act, No 26 of 2005.
- Basic Conditions of Employment Act, No 75 of 1997.
- Broad- Based Black Economic Empowerment Act, No 75 of 1997.
- Business Act, No 71 of 1991; e. Companies Act, No 71 of 2008.
- Compensation for Occupational Injuries & Diseases Act, 130 of 1993.
- Competition Act, No.71 of 2008; h. Constitution of the Republic of South Africa 2008.
- Copyright Act, No 98 of 1978.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 9 of 29	

- Customs & Excise Act, 91 of 1964.
- Electronic Communications Act, No 36 of 2005.
- Electronic Communications and Transactions Act, No 25 of 2002.
- Employment Equity Act, No 55 of 1998.
- Financial Intelligence Centre Act, No 38 of 2001.
- Identification Act, No. 68 of 1997.
- Income Tax Act, No 58 of 1962; q. Intellectual Property Laws Amendment Act, No 38 of 1997.
- Labour Relations Act, No 66 of 1995.
- Long Term Insurance Act, No 52 of 1998.
- Occupational Health & Safety Act, No 85 of 1993.
- Pension Funds Act, No 24 of 1956.
- Prescription Act, No 68 of 1969.
- Prevention of Organized Crime Act, No 121 of 1998.
- Promotion of Access to Information Act, No 2 of 2000.
- Protection of Personal Information Act, No. 4 of 2013.
- Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
- Revenue laws Second Amendment Act. No 61 of 2008.
- Skills Development Levies Act No. 9 of 1999.
- Short-term Insurance Act No. 53 of 1998.
- Trust Property Control Act 57 of 1988
- Unemployment Insurance Contributions Act 4 of 2002.
- Unemployment Insurance Act No. 30 of 1966.
- Value Added Tax Act 89 of 1991.

* This is an indicative list only and by no means a complete list of legislation


* Accessibility of these documents and records may be subject to the grounds of refusal as set out in this Manual.

11. DETAIL TO FACILITATE A REQUEST FOR ACCESS TO A RECORD OF KAEFER (Section 51(1)e)

- 11.1 The requester must comply with all the procedural requirements contained in the Act relating to the request for access to a record.
- 11.2 The requester must complete **Form 2 (Request for Access to Record) in Annexure 1A**, and submit it to the Information Officer. Contact details as shown in 6 above. **This form is available for download on the KAEFER website: www.kaefer.co.za or on request from the Information Officer.**
- 11.3 The prescribed form must be completed and submitted with all the required information
- 11.4 If a request is made on behalf of another person, then the requester must submit proof of the capacity in which the requester is making the request, to the reasonable satisfaction of the Information Officer.
- 11.5 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 10 of 29	

12 REFUSAL OF ACCESS TO RECORDS

KAEFER is entitled to refuse access to information

12.1 Main grounds for refusal relates to:

- a. mandatory protection of the privacy of a third party who is a natural person or a deceased person (section 63) or a juristic person, as included in the POPIA, which would involve the unreasonable disclosure of personal information of that natural or juristic person;
- b. mandatory protection of personal information and for disclosure of any personal information to, in addition to any other legislative, regulatory, or contractual agreements, comply with the provisions of the POPIA.
- c. mandatory protection of the commercial information of a third party (section 64), if the record contains:
 - i. trade secrets of the third party.
 - ii. financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interests of that third party.
 - iii. information disclosed in confidence by a third party to KAEFER if the disclosure could put that third party at a disadvantage in negotiations or commercial competition.
- d. mandatory protection of confidential information of third parties (section 65), if it is protected in terms of any agreement.
- e. mandatory protection of the safety of individuals and the protection of property (section 66).
- f. mandatory protection of records which would be regarded as privileged in legal proceedings (section 67).

12.2 The commercial activities (Section 68), of KAEFER, which may include:


- a. trade secrets of KAEFER.
- b. financial, commercial, scientific, or technical information which disclosure could likely cause harm to the financial or commercial interests of KAEFER.
- c. information which, if disclosed could put KAEFER at a disadvantage in negotiations or commercial competition.
- e. a computer program which is owned by KAEFER, and which is protected by copyright.
- f. the research information of KAEFER or a third party, if its disclosure would disclose the identity of KAEFER, the researcher or the subject matter of the research and would place the research at a serious disadvantage.

12.3 Requests for information that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources shall be refused.

12.4 If a requested record for which access would ordinarily be allowed, cannot be found or if the record does not exist, the Information Officer shall, by way of an affidavit or affirmation, notify the requester.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 11 of 29	

Such a notice will be regarded as a decision to refuse a request for access to the record concerned for the purpose of the Act. If the record should later be found, the requester shall be given access to the record.

13 REMEDIES AVAILABLE WHEN KAEFER REFUSES REQUEST

13.1 Internal Remedies

KAEFER does not have an internal appeals procedure.

The decision made by the Information Officer is final. 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.

13.2 External Remedies

- 13.2.1. A requester/third party that is dissatisfied with the Information Officer's refusal to disclose information, may within 30 (thirty) days of notification of the decision, apply to a Court for relief.

14. ACCESS TO RECORDS HELD BY KAEFER

14.1 Prerequisites for Access by Personal/Other Requester

There are two types of requesters:

a. Personal Requester

- i. A personal requester is a requester who is seeking access to a record containing personal information about him/herself.

In this instance, KAEFER will voluntarily provide the requested information or give access to any record regarding the requester's personal information

b. Other Requester

- i This requester is entitled to request access to Information on a Data Subject.

In considering such a request, the Information Officer will take all reasonable steps to inform the Data Subject, to whom the requested record relates, of the request.

The Data Subject may object in writing to the request or give written consent for disclosure.


15. PRESCRIBED FEES FOR ACCESS TO INFORMATION

These are the fees paid by the requester to KAEFER, to cover the costs of finding and copying the required records.

KAEFER reserves the right to charge a reasonable fee dependent on the size and scope of the request. A quotation will be sent to the requester where applicable.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 12 of 29	

16. DECISION

- 16.1 KAEFER will process the request within 30 (thirty) days unless the requester has stated special reasons to the satisfaction of the Information Officer, that the information is required sooner.

The prescribed time will commence only once the requester has furnished all the necessary and required information.

If circumstances dictate that the 30-day timeline cannot be met, KAEFER will notify the requester in writing, should an extension be sought.

- 16.2 The requester shall be advised whether access is granted/denied in writing, **by completing Form 3 (Outcome of Request and of Fees Payable) in Annexure 1B..**

17. PROTECTION OF PERSONAL INFORMATION THAT IS PROCESSED BY KAEFER

KAEFER needs Personal Information relating to both individual and juristic persons in order to carry out its business and organizational functions. The way this information is processed and the purpose for which it is processed must satisfy certain POPI requirements.

When processing this information, KAEFER needs to ensure that the information:

- a. is processed lawfully, fairly, and transparently. This includes communication to Data Subjects when their data is collected by KAEFER, in the form of consent forms.
- b. is processed only for the purposes for which it was collected.
- c. will not be processed for a secondary purpose unless that processing is compatible with the original purpose.
- d. is adequate, relevant, and not excessive for the purposes for which it was collected.
- e. is accurate and kept up to date.
- f. will not be kept for longer than is necessary.
- g. is processed in accordance with integrity and confidentiality principles; this includes physical and organizational measures to ensure that Personal Information, in both physical and electronic form, are subject to an appropriate level of security when stored, used and communicated by KAEFER, in order to protect against access and acquisition by unauthorized persons and accidental loss, destruction or damage;
- h. is processed in accordance with the rights of Data Subjects, where applicable

17.1 Data Subjects Rights

- a. To be notified that their Personal Information is being collected by KAEFER. The Data Subject also has the right to be notified in the event of a data breach.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL	
<p>Compiled By: R. Mulaudzi</p> <p>Approved By: J. Cleaver</p> <p>Date: 24/10/23</p>	<p>Serial No: QMP 6.2.12</p> <p>Revision: 1</p> <p>Page 13 of 29</p>



KAEFER

- b. To know whether KAEFER holds Personal Information about them, and to access that information. Any request for information must be handled in accordance with the provisions of this Manual.
- c. To request the correction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or unlawfully obtained personal information.
- d. To object to KAEFER's use of their Personal Information and request the deletion of such Personal Information (deletion would be subject to KAEFER's record keeping requirements).
- e. To object to the processing of Personal Information for purposes of direct marketing by means of unsolicited electronic communications.
- f. Be protected under POPI and to institute civil proceedings regarding the alleged noncompliance with the protection of his, her or its personal information.

17.2 Type and Classification of Personal Information Collected by KAEFER

The KAEFER Data Inventory – **Annexure 2**, lists and classifies all personal data collected by the Company

17.3 Purpose of Processing Personal Information

The Purpose of Processing of Personal Information by the Company, is clearly set out in the KAEFER Data Inventory - Annexure 2

17.4 Recipients of Personal Information

KAEFER may provide a Data Subject's Personal Information to:

- a. Any firm, organization, or person that KAEFER uses to collect payments and recover debts or to provide a service on its behalf.
- b. Any firm, organization, or person that/who provides KAEFER with products or services.
- c. Any payment system KAEFER uses.
- d. Regulatory and governmental authorities or ombudsmen, or other authorities, including tax authorities, where KAEFER has a duty to share information.
- e. Third parties to whom payments are made on behalf of employees.
- f. Financial institutions from whom payments are received on behalf of data subjects.
- g. Any other operator not specified.
- h. Employees, contractors, and temporary staff; and
- i. Agents and consultants.


17.5 Cross-border flows of Personal Information

Personal Information may only be transferred out of the Republic of South Africa if the:

- a. recipient country can offer such data at an "adequate level" of protection. This means that its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in POPI; or

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 14 of 29	

- b. Data Subject consents to the transfer of their Personal Information; or
- c. transfer is necessary for the performance of a contractual obligation between the Data Subject and the KAEFER; or
- d. transfer is necessary for the performance of a contractual obligation between KAEFER and a third party, in the interests of the Data Subject; or
- e. the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

The Data Inventory - **Annexure 2**, sets out details of cross-border transfers of Personal Information at KAEFER.

17.6 Obtaining Written Consent

Written consent must always be obtained before personal data is collected from data subjects. This includes employees, suppliers, clients and sub-contractors.

17.6.1 Employees

All job applicants and new hires will be required to sign Consent Forms to allow for the collection, processing and storage of their personal information. The Consent Form will also include confidentiality, to reduce the risk of unauthorised disclosures of personal information which employees process on behalf of KAEFER.

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.

An example of the "Employee Consent and Confidentiality Form" can be seen in **Annexure 3**.

17.6.2 Suppliers

KAEFER will be required to obtain consent from all suppliers in order to collect and process their information. This includes joint ventures, sub-contractor agreements, SLA's, etc.

Procurement Department will be responsible to ensure a copy of the revised Terms and Conditions containing the POPIA requirements and confidentiality aspects, are sent to ALL (existing and future) suppliers and that acknowledgements are kept on file for auditing purposes.


Annexure 4 – Terms and Conditions

17.6.3 Direct Marketing Consent

All forms of direct marketing will be prohibited unless the explicit consent has been obtained from the data subject. The communication department will obtain consent from all Client contacts on the

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 15 of 29	

KAEFER's mailing list and will be responsible to keep the information up-to-date. The database should be updated annually.

See **Annexure 12 - Client Mailing List Consent Form**

17.6.4 Tender Documents

As tender submissions contain private information of the company and individuals, working for KAEFER, the estimating department will be responsible to issue Clients the revised Terms and Conditions, containing POPIA requirements and confidentiality aspects, and ensure that acknowledgements are kept on file for auditing purposes.

See **Annexure 13 – Terms and Conditions.**

17.6.4 CCTV Footage

The Privacy Act states that where CCTV cameras are installed in a workplace, employees should be made aware of this. This should be included in employment contracts as well as outlining the purpose of the CCTV system. - being to secure the premises and not for any other reason. Cameras must be placed in full view, and signs placed in conspicuous areas around the premises which will also serve to alert visitors that they are being recorded.

Cameras may not be placed in private areas such as changing rooms and toilets.

17.6.5 GPS Fleet Tracking

As with CCTV Systems, employees using company vehicles must be alerted to the fact that the vehicle is tracked by the Fleet Management System and the purpose for which the GPS tracking has been installed, being:

- Increased efficiency through streamlined travel for delivery
- Security and recovery as well as insurance requirement
- Monitoring overtime and compliance with labor laws.
- Verifying that time records are accurate; company policies are followed, and employees are engaging in safe behavior.
- If an employee is suspected of wrongdoing, an employer can use GPS tracking as part of its internal investigation of the employee.


17.6.6 Biometric Scanners

Employees must be made aware that, KAEFER makes use of biometric systems to gather fingerprint data for clocking purposes, to ensure payroll accuracy and in some instances used for Security Access.

17.6.7 Photographs, Audio and Video

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 16 of 29	

Written consent must be obtained in the case of persons depicted in photos, video footage and audio voice recordings. This also includes meetings, conferences, training events or training courses (live or online)

The consent of all participants must be obtained at least two working days in advance.

Consent is voluntary, and each participant is completely free to decide whether or not to give it. Only if all participants agree will the recordings be made.

Upon request the employee has the right to inspect the video/audio recording once it is produced.

Annexure 5 is required to be completed when requesting consent.

ALL Signed consent forms must be filed in the relevant person's Personnel File by HR

17.6.8 Photographer's consent

In general, a photographer owns the copyright on the photo taken, as such, consent to use the image for commercial ESF purposes, such as advertising, presentations, brochures or web applications (e.g. social media) will need to be obtained.

The consent forms also include a consent form regarding the copyright of the photographer. This only needs to be completed if it concerns a private recording that was not created as part of normal work activities (example: spouse takes a photo of a jubilee for publication in the K-WERT magazine).

Consent is not required where the photographer is an employee who has been instructed to take the photo/video or if KAEFER has hired an external photographer and therefore signs a written agreement confirming that the rights are with KAEFER.

17.6.9 Consent of the site owner/client

If images/videos are taken on a project site, it is essential to get the site owner's written approval. Only when the consent has been received can photos/videos be taken. If images are used for commercial purposes without the necessary consents, KAEFER may be liable to substantial damages and / or fines.

17.6.10 Media Libraries


Employees should make use of the KAEFER media library when looking for an image or there are many resources online (platforms) where images can be obtained for free or for a low-cost such as behold, or Flickr Creative Commons. or Adobe Stock

Platforms such as Getty images purchase and/or usage rights may be time restricted. If so, the image cannot be used indefinitely or for all communication purposes.

17.7 Objection to the Processing of Personal Information

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi Approved By: J. Cleaver Date: 24/10/23	Serial No: QMP 6.2.12 Revision: 1 Page 17 of 29	

A Data Subject may, at any time object to the Processing of his/her/its Personal Information in the prescribed form as **Annexure 6**, subject to exceptions contained in POPIA.

17.8 Request for correction or deletion of Personal Information

A Data Subject may request for their Personal Information to be corrected/deleted in the prescribed form attached as **Annexure 7** to this Manual

18. AUTOMATED DECISION MAKING

KAEFER does not make use of any automated decision making.


19. PROCEDURE FOR PROCESSING OF PERSONAL INFORMATION BY KAEFER EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF KAEFER

The following rules must be strictly adhered to when processing Personal Information:

- a. All personal information must be treated as a confidential business asset and the privacy of data subjects respected.
- b. Personal Information (unless publicly known), may not directly or indirectly, be utilised, disclosed, or made public in any manner, to any person or third party, either within KAEFER or externally.
- c. To request assistance from the line manager or Information Officer, if unsure about any aspect relating to POPI
- d. Only process personal information where:
 - Explicit written or verbally recorded consent has been granted to the organisation by the data subject, (consent by a legal guardian is necessary for processing data of children under 18)
 - processing is necessary to carry out actions for the conclusion or performance of a contract which the data subject is party
 - The processing complies with an obligation imposed by law
 - The processing protects a legitimate interest of the data subject
 - The processing is necessary for pursuing the legitimate interest of the organisation or of a third party to whom the information is supplied

CONTROLLED DISCLOSURE


When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 18 of 29	

- When the data subject clearly understands for what purpose his/her/its personal information is collected.
- e. 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
- f. KAEFER employees or other persons acting on behalf of KAEFER will under no circumstances:
- Process or access personal information where such processing or access is not a requirement to perform their 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 KAEFER's dedicated server.
 - Share personal information informally.
 - Send personal information electronically via 3rd party applications as this form of communication is not guaranteed to be secure
 - Transfer personal information outside of South Africa without the express permission of the line manager or Information Officer
- g. Ensure 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.
- h.,. Ensure that personal information is encrypted prior to sending or sharing the information electronically outside KAEFER.
- i. Ensure 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.
- j. Ensure that computer screens and other devices are switched off or locked when not in use or when away from their desks.
- k. Terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism e.g.: password protected screensaver
- l. Log off from applications or network services when no longer needed

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi Approved By: J. Cleaver Date: 24/10/23	Serial No: QMP 6.2.12 Revision: 1 Page 19 of 29	

- m. Always maintain clean desktop
- n. Ensuring that where personal information is stored on removable storage medias, that they are securely locked away.
- o. Hard copy records are kept in a secure place where unauthorised persons cannot have access e.g. locked drawer or filing cabinet.
- p. Printers used for personal information printing, should have a pin code function, so the originators are the only ones who can get their printouts and only when standing next to the printer
- q. Ensure that personal information is kept accurate and up to date, by periodically confirming a data subject's details (Employee, Client, Operator). Databases should be updated at least annually.
- r. Where details are outdated, obtain line management's authorisation to update information
- s. Ensure that information is stored only for as long as needed or required in terms of legislation.
- t. Line Management authorisation must be given before deleting or disposing of personal information
- u. Ensure disposal or deleting of information is done in the appropriate manner
- v. When becoming aware of, or there is suspicion of a security breach, such as unauthorised access, interference, alteration, destruction or the unsanctioned disclosure of personal information, report it immediately to the Information Officer.

20. INFORMATION SECURITY

We are legally obliged to provide adequate protection for the personal information we hold and to stop unauthorized access, use or loss of personal information.

A preliminary assessment of the suitability of the information security measures implemented or to be implemented by KAEFER, will be conducted to ensure that the Personal Information processed, is safeguarded.


The assessment of IT Security will require the relevant expertise.

Areas to be assessed and monitored on an ongoing basis are:

- Physical security.
- Computer and network security.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 20 of 29	

- Access to personal information.
- Secure communications.
- Security in contracting out activities or functions.
- Retention and disposal of data.
- Acceptable usage of personal information.
- Governance and regulatory issues.
- Monitoring access and usage of private information.
- Investigating and reacting to security incidents.

20.1 IT Security


In order to secure electronic data, the IT Department will ensure the following:

- IT infrastructure, digital filing systems and any other devices used for processing personal information meet acceptable security standards.
- all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- that servers containing personal information are sited in a secure location, with no unauthorised entry.
- that all electronically stored personal information is backed-up and tested on a regular basis.
- that all back-ups containing personal information are protected from unauthorised access, accidental deletion, and malicious hacking attempts
- that personal information being transferred is electronically encrypted.
- that all servers and computers containing personal information are protected by a firewall and the latest security software
- conduct regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly and verify if information has been accessed by any unauthorised persons
- perform a proper due diligence review prior to contracting operators or any other third-party service provider to process personal information such as cloud computing service

Refer to **IT Governance Rule QMP 5.3.1** for a more in depth look at IT Security at KAEFER

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi Approved By: J. Cleaver Date: 24/10/23	Serial No: QMP 6.2.12 Revision: 1 Page 21 of 29	

20.2 Destruction of Personal Information

All Departments must ensure that personal information is destroyed or deleted in a manner that prevents its reconstruction in an intelligible form. This would apply to both hard copies/documents, as well as electronic versions

Manner of destruction/deletion must be determined and clearly defined on the KAEFER Data Inventory – **Annexure 2**

21. TRAINING

POPI Training and awareness will be conducted at all levels of the organisation:

Information Officers & Deputy Information Officers	External POPI Training
All Staff including Top Management	Internal POPI Training with online assessment
Site Personnel: Administrators/Site Managers/Supervisors/Safety Officers as well	Internal POPI Training with online assessment
All other blue-collar workers	Training through toolbox talks given by Safety Officers and Site IR's
Annual re-training of all employees	Internal POPI Training with online assessment/Toolbox Talks by Safety Officers and Site I/R's
New staff members	Internal POPI Training with online assessment

22. DATA BREACH INCIDENT RESPONSE

22.1 Definition of a Data Breach


The Company's definition of a personal data breach, is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

22.2 Reporting

As soon as a data breach has been identified/suspected, it must be reported to the Line Manager, Information Officer and MD.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 22 of 29	

22.3 Containment Measures

Immediate containment measures must be put in place to secure the information and to limit further leakages or breaches.

22.4 Investigation

All incidents must be thoroughly investigated and recorded regardless of severity or outcome.

A Team appointed by the Information Officer will undertake the investigation and dependent on the findings of the investigation and if necessary, the team will:

- Seek urgent legal advice
- Notify the Data Subject in writing
- Notify the Information regulator in writing
- Prepare a plan of any other actions required to close gaps and prevent similar occurrences

No communication may take place to/or on (the) media or other parties until legal advice has been obtained on how best to communicate regarding the incident.

KAEFER's full co-operation, support and transparency must be given to Data Subject/s and the Information Regulator, especially in terms of any subsequent investigations by the Regulator.

22.5 Record of Breach

Strict records must be kept of ALL data breaches.

The Information Officer will enter all data breaches into the Data Privacy Breach Incident Log - **Annexure 8**.

Investigations will be recorded and closed out on the Data Breach Incident Form – **Annexure 9**

23. DISCIPLINARY ACTION

Where a POPIA/PAIA complaint or infringement investigation has been finalised, KAEFER 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.


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

- Further awareness training in the case of minor negligence
- 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

Disciplinary action will be taken in accordance with the KAEFER Disciplinary Procedure QMS 6.2.5

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi Approved By: J. Cleaver Date: 24/10/23	Serial No: QMP 6.2.12 Revision: 1 Page 23 of 29	

24. POPIA AND PAIA AUDITING

24.1 Internal

The Quality Manager will schedule and undertake periodic POPIA/PAIA audits throughout the Organisation against the set POPIA and PAIA Policies and Procedures. Audits will be conducted in accordance with the Internal Audit Procedure QMS 8.2.2 and NCR's issued in accordance with Preventive and Corrective Procedure QMS 8.5.2

- a. Audit Scope**
Scope will be this Policy
- b. Frequency**
Minimum annually

24.2 External Audits

To ensure compliance, the information Officer may co-ordinate an annual external audit by an expert legal third party.

25. LEGAL REQUIREMENTS

Each Information/Deputy Information Officer will be given a copy of the POPI hand manual for their reference.

A POPI expert legal advisory service will be used to ensure that the Information Officer/s is/are kept up to speed with the latest developments in data/information protection laws, case laws as well as an advisory service and tools.

The Information Officer will communicate any notable changes in legislation to EXCO

26. MANAGEMENT REVIEW

POPIA/PAIA compliance will be discussed and reviewed annually in the Management Review Meetings in accordance with the Management Review Procedures QMS 5.6.


27. DUTIES AND RESPONSIBILITIES

27.1 Exco/MD

Exco cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA and PAIA.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 24 of 29	

Managing Director

Is responsible for:

- a. Appointing capable Information Officer/s
- b. Ensuring sufficient resources are made available for PAIA/POPI such as:
 - Specific Training (Management and Employees that process personal information)
 - Specialist Legal Advice/Legal Update services and periodic audits by external parties
 - Necessary data security products and software
 - IT Security Testing
 - Data archiving systems
- c. Ensure all persons responsible for the processing of personal information on behalf of the organisation:
 - are appropriately trained and supervised to do so.
 - understand they are contractually obligated to protect the information.
 - are aware that wilful or negligent breach of this policy processes and procedure may lead to disciplinary action being taken against them.
- d. Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include approving the amendment to existing agreements.
- e. Discuss PAIA and POPIA in Manco and Exco meetings and record these discussions in minutes of the meetings.
- f. Ensure that POPIA/PAIA is considered in any decision or change in the Organization
- g. Sign off on all related instructions, deviations or policy changes.


27.2 a. Information Officer

Responsible for:

- Taking steps to ensure KAEFER's reasonable compliance with the provisions of POPIA and PAIA
- Keeping Exco informed about all POPIA and PAIA related matters including security breaches
- Keeping abreast of changes in legislation pertaining to POPIA and PAIA in conjunction with the Specialist Legal Advisory service.
- Ensuring that audits are scheduled and conducted on a regular basis

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 25 of 29	

- Ensuring KAEFER makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the organisation
- Ensuring requests for information are handled as stated in this manual.
- Encouraging compliance with the conditions required for the lawful processing of data.
- Assisting the Information Regulator with Investigations and requests

b. Deputy Information Officers

- To assist the Information Officer with responsibilities in a. above, and to stand-in when the Information Officer is not available.
- Deputy Information Officers assigned to a Department, will assist with all Information Officer Duties pertaining to that Department

27.3 Communication Officer

- Maintaining the PAIA and POPIA statements and disclaimers that are displayed on the KAEFER website, including those attached to communications such as emails and electronic newsletters.
- Ensuring consent from Client contact list for the receiving of KAEFER electronic information
- Maintaining correct Client contact information at least annually
- Where necessary working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA.
- Ensure the organisation complies to GDPR in terms of Images/Video/Audio, etc.

27.4 HR Manager


- Consult with employees regarding the Employee POPI consent form
- Obtain documented consent from all KAEFER employees and file in Personnel Files
- Draw up new employment contracts with POPIA requirements for new hires
- Obtain signed consent forms from candidates applying for positions
- Update relevant Job Descriptions to include POPIA and PAIA duties and responsibilities
- Ensure POPIA requirements are met within the HR/IR's area of control

27.5 Procurement Manager

- Ensure all existing and future suppliers receive a copy of the revised Terms and Conditions and acknowledge receipt thereof.
- Ensure all POPIA requirements are met within Procurement's area of control

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 26 of 29	

27.6 Financial Director

In terms of IT the FD is responsible to manage and oversee:

- Assessment of IT Security and ensuring suitable IT Security is in place
- Ensuring IT Audits are conducted periodically and security issues rectified
- Conducting due diligence on third party IT service providers
- Provide IT expertise to assist in Data Breach investigations

Ensure all POPIA requirements are met within Finance and Payroll's area of control

27.7 Quality Manager

- Schedule and conduct PAIA/POPIA Audits
- Make necessary updated/revisions to POPIA/PAIA Manuals, Procedures and Policies
- Maintain the KAEFER Data Inventory

27.8 Estimating Manager

- Ensure Clients receive a copy of the revised Terms and Conditions with every tender submitted and acknowledgement kept on file for verification
- Control and avoid unnecessary copies and duplication of information of Tender Returnable and Client Tender Information
- Ensure suitable destruction of Client Information and Tender Returnable private information when retention period has ended
- Ensure all other POPIA requirements are met within the Estimating and BD area of control

27.9 All HOD's and Line Managers


- Ensure all POPI and PAIA requirements are met within their departments/sites and areas of control

28. 10 PRACTICAL MEASURES FOR COMPLIANCE

- 28.1 Assess current records of personal information
- 28.2 Define the purpose of the information gathering/ processing
- 28.3 Define legal basis
- 28.4 Identify how processed
- 28.5 Audit current process used
- 28.6 Ensure appropriate security safeguards are in place
- 28.7 Verify the quality of the information
- 28.8 Further processing

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 27 of 29	

28.9 Monitor and manage your retention of records and disposal

28.10 Delete unauthorized information

29. FAQ

29.1 What is the aim of the POPI Act?

- Promote the protection of personal information processed by public and private bodies.
- Introduce certain conditions to establish minimum requirements for the processing of personal information.
- Provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of both this Act as well as the Promotion of Access to Information Act, 2000.
- Provide for the issuing of codes of conduct.
- Provide for the rights of persons regarding unsolicited electronic communications and automated decision making; and
- Regulate the flow of personal information across the borders of the Republic.

29.2 What is personal data?

If you hold any of the types of data mentioned below then you need the individual's permission to have possession of it.


- Gender, race, marital status, nationality, sex, mental health, religion, belief, language, etc.
- Education or financial, criminal, medical and employment history.
- Biometrics, including physical, behaviour and/or physiological characterisations (DNA analysis, retinal scanning, blood type, etc.)
- Email address, telephone number, location information, online identifier, etc.
- Correspondence of a private nature.
- Opinions or views that another person has relating to the individual.
- The individual's name, if disclosure of the name would lead to the revealing of information about the individual.

29.3 To whom does POPIA apply?

- Any public or private body, or any other person which, unaided or in combination with others, regulates the purpose of and means for processing personal information (Responsible Party).
- The 'Responsible Party' of every company is accountable for ensuring and enforcing its own compliance.
- Any person who processes personal information for a Responsible Party in terms of a mandate or agreement, without coming under the direct authority of the Responsible Party.

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi	Serial No: QMP 6.2.12	
Approved By: J. Cleaver	Revision: 1	
Date: 24/10/23	Page 28 of 29	

29.4 What happens if I do not comply to the POPI Act?

- If you act recklessly with this information, you not only face regulatory sanctions, but you also run an actual risk of damaging client relationships and overall business reputation.
- Non-compliance may have far-reaching consequences and could expose the Responsible Party to a penalty or fine of R10 million and/or imprisonment of 12 months up to 10 years.

29.5 Who is permitted to be the Information Officer?

- There are no legal requirements for a formal qualification to be obtained by the information Officer, but larger organisations tend to use someone with legal qualifications.
- The Information Officer can be a full-time or part-time role, depending on the company's size and requirements.

29.6 Do I have to notify the Regulator of any Data Breaches?

- Yes.
- Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the responsible party must notify the Regulator
- Any number of breaches requires a notification to the Regulator, including just one minor breach.
- If data on a device is encrypted then the theft of the device does not need to be notified to the Regulator, but without encryption a cell phone, tablet, laptop, or computer theft needs to be registered with the Regulator.

29.7 When does the POPI Act kick off?

On the 1st July 2021


30. AVAILABILITY AND UPDATING OF THIS MANUAL

This PAIA/POPI Manual, KAEFER Privacy Policy, **Request Form 02: Request for Access to Record and Form 3 Outcome of request and of fees payable**, will be available on the web site www.kaefer.co.za and at the KAEFER Head Office Premises.

This manual will be reviewed annually in the Management Review Meeting and revised when necessary

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

PAIA AND POPIA POLICY MANUAL		
Compiled By: R. Mulaudzi Approved By: J. Cleaver Date: 24/10/23	Serial No: QMP 6.2.12 Revision: 1 Page 29 of 29	

31. CHANGE TRACKING HISTORY

Rev. 0 - 18/05/2021 Issued for implementation
 Rev. 1 - 24/10/2023 Change of Annexures

32. ANNEXURES

Annexure No.	Doc. No.	Title
Annexure 1A	FORM 2	Request for access to Record
Annexure 1B	FORM 3	Outcome of Request and of Fees Payable
Annexure 2	KTQ 237	KAEFER Data Inventory
Annexure 3	KTQ 240	Employee Consent and Confidentiality Clause
Annexure 4	KTQ 242	General Terms and Conditions for Purchase of Goods and Services
Annexure 5	KTQ 234	KAEFER Video/Photo/Audio Consent Form
Annexure 6	FORM 1	FORM 1 – Objection to the processing of personal information
Annexure 7	FORM 2	FORM 2 – Request for correction or deletion of personal information
Annexure 8	KTQ 236	Data Privacy Breach Incident Log
Annexure 9	KTQ 239	Data Breach Incident Investigation Form
Annexure 10	KTQ 242	Designation and Delegation of Authority to the Information Officer
Annexure 11	KTQ 241	Designation and Delegation of Authority to the Deputy Information Officer
Annexure 12	KTQ 243	Client Mailing List Consent Form
Annexure 13	KTQ 244	General Terms and Conditions for supply of goods and services

CONTROLLED DISCLOSURE

When downloaded from the Management System this document is uncontrolled and the responsibility rests with the user to ensure it is the most current version

FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. Proof of identity must be attached by the requester.
2. If requests made on behalf of another person, proof of such authorisation, must be attached to this form.

TO: The Information Officer

(Address)

E-mail address:

Fax number:

Mark with an "X"

Request is made in my own name

Request is made on behalf of another person.

PERSONAL INFORMATION			
Full Names			
Identity Number			
Capacity in which request is made <i>(when made on behalf of another person)</i>			
Postal Address			
Street Address			
E-mail Address			
Contact Numbers	Tel. (B):		Facsimile: <input type="text"/>
	Cellular:		
Full names of person on whose behalf request is made <i>(if applicable):</i>			
Identity Number			
Postal Address			

Street Address			
E-mail Address			
Contact Numbers	Tel. (B)		Facsimile
	Cellular		
PARTICULARS OF RECORD REQUESTED			
<i>Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)</i>			
Description of record or relevant part of the record:			
Reference number, if available			
Any further particulars of record			
TYPE OF RECORD <i>(Mark the applicable box with an "X")</i>			
Record is in written or printed form			
Record comprises virtual images <i>(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)</i>			
Record consists of recorded words or information which can be reproduced in sound			
Record is held on a computer or in an electronic, or machine-readable form			

FORM OF ACCESS
(Mark the applicable box with an "X")

Printed copy of record (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)	
Written or printed transcription of virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc)	
Transcription of soundtrack (written or printed document)	
Copy of record on flash drive (including virtual images and soundtracks)	
Copy of record on compact disc drive (including virtual images and soundtracks)	
Copy of record saved on cloud storage server	

MANNER OF ACCESS
(Mark the applicable box with an "X")

Personal inspection of record at registered address of public/private body (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format (including transcriptions)	
E-mail of information (including soundtracks if possible)	
Cloud share/file transfer	
Preferred language (Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED

If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.

Indicate which right is to be exercised or protected	

Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a)	<i>A request fee must be paid before the request will be considered.</i>
b)	<i>You will be notified of the amount of the access fee to be paid.</i>
c)	<i>The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.</i>
d)	<i>If you qualify for exemption of the payment of any fee, please state the reason for exemption</i>
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	Facsimile	Electronic communication <i>(Please specify)</i>

Signed at _____ this _____ day of _____ 20 _____

Signature of Requester / person on whose behalf request is made

FOR OFFICIAL USE

Reference number:	
Request received by: <i>(State Rank, Name And Surname of Information Officer)</i>	
Date received:	
Access fees:	
Deposit (if any):	

Signature of Information Officer

FORM 3
OUTCOME OF REQUEST AND OF FEES PAYABLE
 [Regulation 8]

Note:

1. If your request is granted the—
 - (a) amount of the deposit, (if any), is payable before your request is processed; and
 - (b) requested record/portion of the record will only be released once proof of full payment is received.
2. Please use the reference number hereunder in all future correspondence.

Reference number: _____

TO: _____

Your request dated _____, refers.

1. You requested:

Personal inspection of information at registered address of public/private body (<i>including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form</i>) is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you. If you then require any form of reproduction of the information, you will be liable for the fees prescribed in Annexure B.	
---	--

OR

2. You requested:

Printed copies of the information (<i>including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form</i>)	
Written or printed transcription of virtual images (<i>this includes photographs, slides, video recordings, computer-generated images, sketches, etc</i>)	
Transcription of soundtrack (<i>written or printed document</i>)	
Copy of information on flash drive (<i>including virtual images and soundtracks</i>)	
Copy of information on compact disc drive (<i>including virtual images and soundtracks</i>)	
Copy of record saved on cloud storage server	

3. To be submitted:

Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format (<i>including transcriptions</i>)	
E-mail of information (<i>including soundtracks if possible</i>)	
Cloud share/file transfer	
Preferred language: <i>(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)</i>	

Kindly note that your request has been:

Approved

Denied, for the following reasons:

--

4. Fees payable with regards to your request:

Item	Cost per A4-size page or part thereof/item	Number of pages/items	Total
Photocopy			
Printed copy			
For a copy in a computer-readable form on:			
(i) Flash drive	R40.00		
• To be provided by requestor			
(ii) Compact disc	R40.00		
• If provided by requestor			
• If provided to the requestor	R60.00		
For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on the quotation of the service provider		
Copy of visual images			
Transcription of an audio record, per A4-size	R24.00		
Copy of an audio record			
(i) Flash drive	R40.00		
• To be provided by requestor			
(ii) Compact disc	R40.00		
• If provided by requestor			
• If provided to the requestor	R60.00		
Postage, e-mail or any other electronic transfer:	Actual costs		
TOTAL:			

5. Deposit payable (if search exceeds six hours):

Yes

No

Hours of search	Amount of deposit (calculated on one third of total amount per request)

The amount must be paid into the following Bank account:

Name of Bank: _____
 Name of account holder: _____
 Type of account: _____
 Account number: _____
 Branch Code: _____
 Reference Nr: _____
 Submit proof of payment to: _____

Signed at _____ this _____ day of _____ 20 _____

 Information officer