

## CFA SOCIETY OF SOUTH AFRICA

### POPIA COMPLIANCE MANUAL

VERSION 1.0

#### Table of Contents:

1. Introduction
2. Scope
3. Information Officer
4. Duties and Responsibilities
5. Definitions
6. Responsibilities
7. Data Processing Principles
8. Records Available on Request
9. Records Available Without a Request
10. Records Available in Accordance With Any Other Legislation
11. Request for Access to Information
12. Refusal of Access to Records
13. Decision
14. Remedies for Refusal of a Request for Access
15. Access to Records
16. General Description of Information Security Measures
17. Availability and Updating of POPIA Manual

## 1. Introduction:

The Protection of Personal Information Act (POPIA) is a South African law designed to regulate the processing of personal information and to ensure the protection of individuals' privacy rights. This manual serves as a guide for CFA Society South Africa to ensure compliance with the Protection of Personal Information Act, 4 of 2013 ("POPIA").

### **CFA Society South Africa**

2011/011107/08

**Address:** Network Spaces  
The Pivot  
Block E  
Montecasino Boulevard  
Fourways  
Johannesburg

**Telephone:** 010 011-9066

**Website:** [www.cfa.ac.za](http://www.cfa.ac.za)

## 2. Scope:

This manual applies to all employees, contractors, and third parties who process personal information on behalf of CFA Society South Africa.

2.1. Provide guidance on the type of records that the CFA Society South Africa ("CFA Society") holds that are accessible without making a formal request.

2.2 Provide a description of the data subjects on which CFA Society has records and the types of records kept demonstrating that you have a sufficient understanding of how to request access to a record.

2.3 Be aware of the details of the CFA Society records that are accessible in compliance with any other laws.

2.4 Access the information officer's and deputy information officer's complete contact information so they assist with information requests.

# POPIA MANUAL

2.5 Determine if CFA Society will process personal information, its intended use, and a description of the types of data subjects and the information or categories of information they may contain.

2.6 Understand the descriptions of the different types of data subjects and the various categories of information that pertain to them.

2.7 Determine the recipients or groups of recipients to whom the personal information may be provided, and whether CFA Society intends to transfer or handle personal information outside the Republic of South Africa.

2.8 Determine if CFA Society has the necessary security measures in place to guarantee the privacy, reliability, and accessibility of the personal data that will be processed.

2.9 Explain the circumstances where POPIA expressly states that the records containing certain information may not be released.

2.10 Explain that "processing" of personal information refers to any operations that involve handling data, whether manually or automatically, from the point at which it is collected until it is deleted.

## 3. Information Officer

Every responsible party identified in POPIA will have a CEO who will serve as the organization's information officer by default. The CEO of CFA Society South Africa may designate another CFA Society member as the information officer. One or more deputy information officers may be appointed by the information officer in writing.

**CFA Society South Africa appointed the following information officers:**

<b>Information Officer:</b>	<b>Linda Hawkins</b>
<b>Address:</b>	Network Spaces The Pivot Block E Montecasino Boulevard Fourways Johannesburg
<b>Telephone:</b>	011 011-9066 082 563-1608

**Email:** [linda@cfa.ac.za](mailto:linda@cfa.ac.za)

**Deputy Information Officer:** **Thando Mlambo**

**Address:** Network Spaces  
The Pivot  
Block E  
Montecasino Boulevard  
Fourways  
Johannesburg

**Telephone:** 011 011-9066  
073 529-9617

**Email:** [admin@cfa.ac.za](mailto:admin@cfa.ac.za)

## 4. Duties and Responsibilities

4.1. The duties and responsibilities of the information officer include, amongst others:

- 4.1.1 to confirm that the individual is properly registered as the information officer with the office of the information regulator.
- 4.1.2 to guarantee and promote adherence to POPIA's requirements within CFA Society.
- 4.1.3 to respond to any enquiries about POPIA that CFA Society receives.
- 4.1.4 to work with the information regulator's office on any investigations related to CFA Society that are carried out in accordance with Chapter 6 of POPIA.

4.2. To ensure that:

- 4.2.1 a privacy compliance framework is created, put into place, followed, and maintained.
- 4.2.2 the requirements for the authorized processing of personal information are met.

# POPIA MANUAL

4.2.3 a personal information impact assessment is carried out.

4.2.4 a manual is created, followed, maintained, and made available as required by POPIA.

4.2.5 internal controls are created together with functional systems to handle requests for information or access thereto.

4.2.6 internal training sessions are held covering POPIA's rules, codes of behaviour, and information collected from the regulator. Additionally, copies of the manual are made available to anybody upon request.

4.3. The duties and responsibilities of the deputy information officers include, amongst others:

4.3.1 to own, maintain and monitor compliance with this Policy.

4.3.2 report periodically to the information officer and the Risk Steering Committee on the posture of the data privacy framework.

4.3.4 to lead the development of training and awareness materials, with support from other departments and support functions.

4.3.5 to oversee the delivery of training and deployment of awareness sessions. to be easily accessible to all employees.

4.4. To maintain all the documentation required by POPIA which will amongst others include documenting:

4.4.1 the purpose of processing applicable personal information.

4.4.2 the categories of data subjects on which personal information is processed.

4.4.3 the categories of personal information that is processed.

4.4.4 any possible recipients of personal information.

4.4.5 whether personal information is transferred cross-border and the safeguards put into place for the data transferred.

4.4.6 a general description of security measures in place in relation to personal information being processed.

- 4.5. To develop in-depth knowledge of the data processing activities within CFA Society.
- 4.6. To provide advice on projects which have privacy considerations and oversee privacy impact assessments.
- 4.7. To perform, with the support of the information officer and internal audit regular audits to determine compliance to this policy and POPIA.
- 4.8. To ensure consistency in the deployment of the data privacy framework across CFA Society.

## 5. Definitions:

**Personal Information:** Any information relating to an identifiable, living natural person or juristic person.

**Processing:** Any operation or activity performed on personal information.

**Data Subject:** The individual to whom the personal information relates.

**Consent:** Voluntary, specific, and informed expression of will.

**Data Breach:** A security incident that results in the unauthorized access, disclosure, or destruction of personal information.

## 6. Responsibilities:

**Management:** Responsible for implementing and maintaining POPIA compliance measures.

**Employees:** Responsible for adhering to POPIA requirements in their daily activities.

**Data Information Officer (DIO):** Responsible for overseeing POPIA compliance and acting as a point of contact for data subjects and regulatory authorities.

## 7. Data Processing Principles:

**Lawfulness:** Personal information must be processed lawfully and in a manner that respects the privacy of data subjects.

# POPIA MANUAL

**Purpose Specification:** Personal information must be collected for specified, explicit, and legitimate purposes.

**Data Minimisation:** Only necessary personal information should be collected and processed.

**Accuracy:** Personal information must be accurate, complete, and kept up to date.

**Storage Limitation:** Personal information should be kept in a form that permits identification of data subjects for no longer than necessary.

**Integrity and Confidentiality:** Personal information must be secured against unauthorized access, disclosure, or destruction.

## 8. Records Available on Request

8.1 The following records are kept by CFA Society and may only be obtained upon requests:

<b>Records</b>	<b>Subject</b>
<b>Company registration records</b>	Documents of incorporation Memorandum of incorporation Details of company ownership
<b>Financial records</b>	Accounting records Annual financial reports Annual financial statements Asset registers Bank statements Banking details and bank accounts Banking records Debtors / creditors statements and invoices General ledgers and subsidiary ledgers General reconciliation Invoices Paid cheques Policies and procedures Rental agreements Tax returns
<b>Income tax records</b>	PAYE records

# POPIA MANUAL

<b>IT Records</b>	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 System documentation and manuals
<b>Natural Person</b>	Personal information collected by CFA Society may include: Data subjects: <ul style="list-style-type: none"> <li>• Name</li> <li>• Contact details</li> <li>• Identity number</li> <li>• Gender</li> <li>• Dietary requirements</li> </ul>
<b>Human resources</b>	HR policies and procedures Advertised posts Employee records Qualifications Gender Race
<b>Strategic documents, plans and proposals</b>	Annual reports Strategic plans Annual performance plans
<b>Juristic person / entities</b>	Names of contact persons Names of legal entities Physical and postal addresses Contact details Financial information Registration numbers Founding documents Tax related information Authorised signatories Beneficiaries Ultimate beneficial owners

## 9. Records available without a request

9.1 The following records are accessible in accordance with POPIA without completing the required form:

9.1.1 record with a public purpose.

9.1.2 documents made available on the CFA Society website.

9.1.3 unrestricted reports.

9.1.4 statutory records, like those kept by the CIPC.

9.1.5 other non-confidential documents like brochures, newsletters, and the like.

9.2 The information officer must be contacted with requests for these records.

## 10. Records available in accordance with any other legislation

10.1 Records that must be made available under these Acts must be made available for inspection by interested parties in accordance with the terms and conditions of POPIA, the afore-mentioned legislation, and applicable internal policies and procedures, should such interested parties be entitled to such information, unless disclosure is prohibited by law, regulation, contractual agreement, or other means.

10.2 A request for access must be submitted in conformity with POPIA's guidelines.

10.3 CFA Society keeps records according to the following legislation:

10.3.1. Basic Conditions of Employment Act, 75 of 1997.

10.3.2. Broad-Based Black Economic Empowerment Act, 53 of 2003.

10.3.3. Companies Act, 71 of 2008.

10.3.4. Compensation for Occupational Injuries & Diseases Act, 130 of 1993.

- 10.3.5. Competition Act, 71 of 2008.
- 10.3.6. Constitution of the Republic of South Africa, 2008.
- 10.3.7. Copyright Act, 98 of 1978.
- 10.3.8. Electronic Communications Act, 36 of 2005.
- 10.3.9. Employment Equity Act, 55 of 1998.
- 10.3.10. Electronic Communications and Transactions Act, 25 of 2002.
- 10.3.11. Financial Advisory and Intermediary Services Act. 37 of 2002
- 10.3.12. Financial Intelligence Centre Act, 38 of 2001.
- 10.3.13. Health Professions Act, 56 of 1974.
- 10.3.14. Identification Act, 68 of 1997.
- 109.3.15 Income Tax Act, 58 of 1962.
- 10.3.16 Intellectual Property Laws Amendment Act, 38 of 1997.
- 10.3.17. Labour Relations Act, 66 of 1995.
- 10.3.18. Medical Schemes Act, 131 of 1998.
- 10.3.19. National Health Act, 61 of 2003.
- 10.3.20. Occupational Health & Safety Act, 85 of 1993.
- 10.3.21. Pension Funds Act, 24 of 1956.
- 10.3.22. Prescription Act, 68 of 1969.
- 10.3.23. Prevention of Organised Crime Act, 121 of 1998.
- 10.3.24. Promotion of Access to Information Act, 2 of 2000.
- 10.3.25 Protection of Personal Information Act, 4 of 2013.
- 10.3.26. Regulation of Interception of Communications and Provision of Communication Related Information Act, 70 of 2002.
- 10.3.27 Unemployment Insurance Act, 30 of 1996.

## 10.3.28. Value Added Tax Act, 89 of 1991.

Although every effort has been made to present a thorough list of applicable laws, this list may be lacking. To achieve this, this list will be updated as and when CFA Society learns new facts to that effect. To provide the information officer the chance to take the request into account, the requester must specify what legal right the request is based on if they believe that another piece of legislation not mentioned above confers a right of access to a record.

10.4 The grounds of rejection listed in this manual may apply to the accessibility of documents and records requested because of other legislation.

## 11. Request for access to information

11.1 The requester is required to adhere to all the procedural guidelines set forth in this document with regard to the information access request.

11.2 The requester must fill out the prescribed form, which is accessible on the CFA Society website

11.3 The required form must be filled out with enough details to allow the information officer to identify:

11.3.1 the information or records requested.

11.3.2 the identity of the requester.

11.3.3 the form of access required.

11.3.4 the postal address or email address of the requester in the Republic, or if the requester wishes to be informed of the decision in a different manner (in addition to written), the manner and particulars thereof, and

# POPIA MANUAL

11.3.5 the right which the requester is seeking to exercise or protect with an explanation of the reason the record is required to exercise or protect the right.

11.4 Unless the requester provides the information officer with specific justifications that demonstrate an urgent need for the information, CFA Society will process the request within 21 business days.

11.5. If access is allowed or denied, the requester will be informed in writing.

11.6. The information officer will also give reasons for the decision.

11.7. If a request is submitted on someone else's behalf, the requester must provide sufficient documentation to the information officer to prove their authority (section 53 of POPIA)

11.8. If someone is illiterate or disabled and cannot fill out the required form, they may still submit their request verbally.

11.9. If any of the information specified in paragraph 8.3 is missing, the process will be postponed until the missing information is provided.

11.10. The requester must first provide the necessary information before the specified time periods can start.

11.11. If practicable, the information officer will divide the information into sections and only permit the requester access to those sections.

## **12. Refusal of access to records**

12.1. In accordance with POPIA, CFA Society has the right to reject a request for information.

12.2. The reasons for refusal may apply to information access.

12.3. Records that a third party deems confidential will, among other things, require consent from that third party in addition to the usual conditions before access may be granted.

12.4. The following are the primary reasons why CFA Society will deny a request for information:

12.4.1. if the records are classed as special personal information under section 26 of POPIA, processing of such information must be prohibited.

# POPIA MANUAL

- 12.4.2. mandatory protection of personal information and for disclosure of any personal information to comply with POPIA's requirements in addition to any other laws, regulations, or contracts.
- 12.4.3. mandatory protection of personal information and for disclosure of any personal information, and
- 12.4.4. mandatory protection of the privacy of a third party who is a natural person, a deceased person, or a juristic person, as defined by POPIA.
- 12.4.5. trade secrets belonging to a third party.
- 12.4.6. information in the fields of finance, business or technology whose disclosure may adversely affect a third party's financial or economic interests.
- 12.4.7. information that a third party has provided to CFA Society in confidence if the information could harm that third party's position in negotiations or commercial competition.
- 12.5. Information requests that are pointless, vexatious, or require an inappropriate use of resources must be declined.
- 12.6. All information requests will be evaluated on their own merits and in accordance with the relevant legal guidelines and laws.
- 12.7. The information officer must inform the requester that access to a requested record
- 12.8. cannot be granted if the record cannot be located or does not exist.
- 12.9. For the purposes of POPIA, such a notice will be taken as a decision to deny a request for access to the relevant record. If the record is later discovered, unless the information officer denies access to such record, the requester will be granted access to the record in the manner specified by the requester in the required form.
- 12.10. If the disclosure would violate a third party's duty of confidentiality.
- 12.11. If the information would put someone's life or bodily safety at risk.
- 12.12. If the disclosure is illegal under the Criminal Procedure Act, If the information is protected by a third-legal party's privilege or confidential research.
- 12.13. Whenever a disclosure could jeopardize an ongoing investigation or legal action.

12.14. Where the record contains information around crime prevention, detection and prosecution of alleged offenders.

## 13. Decision

13.1. CFA Society will decide within 20 working days whether to approve or deny the request for access to information and will provide written notification along with reasons for either decision.

13.2. If the request is for a substantial amount of information or necessitates a search for information held at another location and the information cannot reasonably be obtained within the initial 20 working day period, CFA Society may extend the 20-business day period for a further period of not more than 30 working days.

13.3 If an extension is requested, CFA Society will inform the requester in writing. Internal

## 14. Remedies for refusal of a request

### 14.1. Internal Remedies

14.1.1 CFA Society does not have an additional internal appeal process and the Information Officer's decision is considered final.

14.1.2. if the request for information is denied and the requester is dissatisfied with the information officer's decision, they will need to pursue external remedies.

### 14.2. External Remedies

A responsible party or data subject may, in terms of section 63(3) of POPIA, submit a complaint to the regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of the information officer.

## 15. Access to Records

15.1 Every procedural requirement of POPIA pertaining to a request for access to a record must be followed by the requester.

15.2 Either of the attached forms must be filled out and sent to the CFA Society information officer or his/her Deputy at the postal or physical address, email address specified in the manual to seek information.

15.3 Records held by CFA Society may only be accessed upon written request on the prescribed form and after all necessary conditions have been satisfied.

15.4. Any person who requests access to information is considered a requester.

15.5. Two categories of requesters exist:

### 14.5.1. Individual Requester

15.5.1. A person who makes a personal request is someone who wants access to information that includes their personal information.

15.5.2. The requested information will be willingly provided by CFA Society, and any records pertaining to the requester's personal information will be made accessible.

### 15.6. Other Requester

15.6.1. The requester has the right to ask for access to data on third parties.

15.6.2. The information officer will use all reasonable efforts to notify the third party to whom the sought record pertains of the request before granting it.

15.6.3. The information officer will let the third party know that he or she can object to the request in writing or orally, or, if necessary, offer written authorization for the disclosure of the information.

15.6.4. The requester must meet the conditions or prerequisite requirements.

## 16. General description of information security measures

16.1. CFA Society employs up to date technology to ensure the confidentiality, integrity and availability of the personal information under its care. Measures include:

16.1.1. firewalls.

16.1.2. virus protection software and update protocols.

16.1.3. secure access control.

16.1.4. secure setup of hardware and software making up the IT infrastructure.

16.1.5. outsourced service providers who process personal information on behalf of CFA Society are contracted to implement security controls.

16.1.6. Non-Disclosure agreements.

## 17. Availability and updating of POPIA manual

17.1. This manual is available for inspection, on reasonable prior notice, free of charge, at the registered address stated herein and further published on CFA Society's website.

17.2 CFA Society may update this manual periodically or as and when applicable legislation change. An updated version of this manual may be requested from the information officer of CFA Society, whose contact details are available on our website.

**CFA SOCIETY SOUTH AFRICA 2024**