PROTECTION OF PERSONAL INFORMATION POLICY

	NAME	DESIGNATION	DATE
Reviewed	Andrew Davies	Information Officer	July 2022
Approved	Executive Committee	Executive Committee	March 2021
Reviewed	Vicky Commaille	Group Company Secretary	March 2021
Compiled	Andrew Davies	Information Officer	March 2021

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA"). POPIA requires Grindrod to inform data subjects as to how their personal information is used, disclosed and destroyed. Grindrod is committed to compliance with POPIA and other applicable legislation, protecting the privacy of data subjects and ensuring that their personal information is used appropriately, transparently and securely.

2. PURPOSE

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

- Breaches of confidentiality
- Failing to offer choice to data subjects to choose how and for what purpose their information is used
- Reputational damage

The policy also demonstrates Grindrod's commitment to protecting the privacy rights of data subjects in the following manner:

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

3. POLICY APPLICATION

This policy and its guiding principles applies to:

- Grindrod's governing body
- All subsidiaries, divisions and business units of Grindrod
- All employees
- All contractors, suppliers and other persons acting on behalf of Grindrod

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as Grindrod's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is a processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa.

4. DEFINITIONS

4.1 Personal information

Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an existing, identifiable juristic person and may include but is not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person
- Information relating to the education or the medical, financial, criminal or employment history of the person
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- The biometric information of the person
- The personal opinions, views or preferences of the person
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence
- Information regarded as confidential business information
- The views or opinions of another individual about the person
- The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

4.2 Data subject

This refers to the natural or juristic person to whom personal information relates, such as employees, clients, delegates, sub-contractors or a company that supplies Grindrod with goods or services.

4.3 Responsible person

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

4.4 Operator

An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the Grindrod to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

4.5 Information Officer

The Information Officer is responsible for ensuring Grindrod's compliance with POPIA. Where no Information Officer is appointed, the Chief Executive Officer will be responsible for performing the Information Officer's duties. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

4.6 Processing

The act of processing information includes any activity or set of operations concerning personal information and includes:

- The collection, receipt, capturing, collation, storage, updating, retrieval, alteration or use
- Dissemination by means of transmission, distribution or making available in any other form
- Merging, linking, erasure or destruction of information

4.7 Record

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

- Writing on any material
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means
- Book, map, plan, graph or drawing
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced

4.8 Consent

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

4.9 Direct marketing

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

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject
- Requesting the data subject to make a donation of any kind for any reason

4.10 Biometrics

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

5. RIGHTS OF DATA SUBJECTS

Grindrod will ensure that it makes data subjects aware of their rights as appropriate and specifically with regards to the following:

5.1 The right to access personal information

Data subjects have the right to establish whether Grindrod holds personal information related to them, including the right to request access to that personal information.

5.2 The right to have personal information corrected or deleted

Data subjects also have the right to ask Grindrod to update, correct or delete their personal information on reasonable grounds.

5.3 The right to object to the processing of personal information

Data subjects have the right on reasonable grounds to object to the processing of their personal information. Grindrod will consider such requests and the requirements of POPIA and may cease to process such personal information and may, subject to statutory and contractual record keeping requirements, also destroy the personal information.

5.4 The right to object to direct marketing

Data subjects have the right to object to their personal information being used for the purposes of direct marketing by means of unsolicited electronic communications.

5.5 The right to complain to the Information Regulator

Data subjects have the right to submit a complaint to the Information Regulator regarding infringements of any of their rights protected under POPI and to institute civil proceedings against alleged non-compliance with the protection of their personal information.

5.6 The right to be informed

Data subjects have the right to be informed that their personal information is being collected by Grindrod and should also be notified in any situation where Grindrod reasonably believes that the personal information of data subjects has been accessed by unauthorised person / s.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of Grindrod will be subject to the following guiding principles:

6.1 Accountability

Compliance failure could damage the reputation of Grindrod or expose Grindrod to a civil claim for damages. The protection of personal information is therefore everybody's responsibility. Grindrod will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. Grindrod will take appropriate steps including disciplinary action against individuals who through intentional or negligent actions and/or omissions fail to comply with this policy.

6.2 Processing limitation

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

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

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

6.3 Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Where the secondary purpose is not compatible with the original purpose, Grindrod will first obtain additional consent from the data subject.

6.4 Information quality

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

6.5 Security safeguards

Section 19 of POPIA requires the adequate protection of personal information that is held by Grindrod. Grindrod will continuously review security controls and processes to prevent unauthorised access and use of personal

information and will put in place the following procedures to ensure the adequate protection of personal information:

- Grindrod's Information Officer whose details are available below is responsible for compliance with the conditions and provisions of POPIA
- Employees will be trained on this policy and POPIA
- Each new employee will be required to sign an employment contract that contains relevant consent and confidentiality clauses for the use and storage of personal information, in terms of POPIA
- Every employee currently employed within Grindrod will be required to sign an addendum to their employment contract, containing relevant consent and confidentiality clauses for the use and storage of personal information, in terms of POPIA
- Redundant hardcopies of personal information are stored in locked bins until it is securely destroyed by our service provider
- Archived personal information are destroyed according to legislative retention periods
- Grindrod's internal server hard drives are protected by firewalls
- The backup of electronic files and data are managed and regulated through a service level agreement entered into with a reputable service provider

7. INFORMATION OFFICERS

Grindrod's Information Officer is Andrew Davies (informationofficer@grindrod.com). The Information Officer is responsible for ensuring compliance with POPIA and has been duly registered with the South African Information Regulator. Deputy Information Officers are appointed to assist the Information Officer.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Board of Directors

Grindrod's Board of Directors is ultimately accountable for ensuring that Grindrod meets its obligations under POPIA. The Board of Directors may, however, delegate some of its responsibilities to management or other capable individuals.

8.2 Information Officer

Grindrod's Information Officer is responsible for:

8.2.1 Encouraging Grindrod's compliance with the conditions for the lawful processing of personal information.
8.2.2 Dealing with requests made to Grindrod pursuant to POPIA.
8.2.3 Working with the Information Regulator in relation to investigations.
8.2.4 Otherwise ensuring compliance by Grindrod with the provisions of POPIA.
8.2.5 Ensuring a compliance framework is developed, implemented, monitored and maintained.
8.2.6 Conducting personal information impact assessments to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
8.2.7 Developing, monitoring, maintaining and making available Grindrod's PAIA manual.
8.2.8 Ensuring internal measures are developed together with adequate systems to process requests for information or access.
8.2.9 Conducting internal POPIA awareness sessions.

8.3. Group Information Technology Manager

Grindrod's Group Information Technology Manager is responsible for:

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

8.4. Group Marketing Manager and Group Brands

Grindrod's Group Marketing Manager and Group Brands are responsible for:

8.4.1 Maintaining the protection of personal information statements and disclaimers that are displayed on Grindrod's website, including those attached to communications such as emails and electronic newsletters.
8.4.2 Addressing any personal information protection queries from media.
8.4.3 Work with persons acting on behalf of Grindrod to ensure that any outsourced marketing initiatives comply with POPIA.

8.5. Group Human Resources Manager

Grindrod's Group Human Resources Manager is responsible for:

8.5.1 Ensuring that the human resource and payroll system is POPIA compliant.
8.5.2 Providing assurance of good privacy practices applied in human resources.
8.5.3 Authorising access rights to the human resource and payroll systems.

8.6. Divisional Chief Executives

Divisional Chief Executives are accountable for ensuring that their division/s meets its obligations under POPIA and will annually sign a POPIA Assurance Letter to this effect.

8.7 Employees and Other Persons Acting on Behalf of Grindrod

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

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

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

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

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

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

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

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks
- Ensuring that where personal information is stored on removable storage medias such as external drives that these are kept locked away securely when not being used
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected
- Undergoing POPI Awareness training from time to time

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

9. DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA infringement investigation has been finalised, Grindrod may recommend any appropriate administrative, legal and / or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy. In the case of ignorance or minor negligence, Grindrod will undertake to provide further awareness training to the employee.

Any gross negligence or intentional mismanagement of personal information will be considered a serious form of misconduct under Grindrod's Disciplinary code and may lead to dismissal.

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

- A recommendation to commence with disciplinary action
- A referral to law enforcement agencies for criminal investigation