GWK GROUP POPIA POLICY

Title	GWK Group PoPIA Policy
Custodian	Group Financial Director
Prepared by	Legal
Location	GWK Intranet and Website
Date approved	9 December 2021
Effective date	9 December 2021
Approved by	GWK Limited's Board of Directors
Revision	30 November 2022

PREAMBLE

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 aims to promote the protection of privacy through providing principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, the GWK Group is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, the GWK Group is committed to effectively managing personal information in accordance with POPIA's provisions.

The Policy is made available on the GWK website www.gwk.co.za and by request from GWK head office.

Table of Contents **Pg**

1. POLICY PURPOSE

1.1 Statement and purpose

1.1.1 The value of information as an asset to the GWK Group of companies, comprising GWK Ltd and all its subsidiaries, cannot be underestimated. The ever-increasing dependence of GWK on information systems creates a unique vulnerability for our organisation, requiring the introduction of business rules to provide clear and definitive instructions to assist GWK in securing its information.

1.1.2 The term "information security" refers to the management of the integrity, availability and confidentiality of the lifeblood of our organisation, which includes business trade secrets, contractual relationships, intellectual property, financial and operational systems, client and transaction details and information published to the public.

1.1.3 A breach in information security may compromise GWK's ability to provide goods or services, be the cause of losses in revenue through fines or penalties and fraud, destruction of proprietary or confidential data, lead to breaches of business contracts, trade secrets and privacy or damage our reputation with our stakeholders.

1.1.4 Information security is regarded as a critical part of GWK risk management programmes. This policy provides a framework for the safeguarding of our organisational information, compliance with relevant legislation and to serve as reference documents for internal quality control processes.

1.1.6 The responsibility to preserve GWK's information security is not limited to the IT department, but requires the co-operation of every employee. This policy has accordingly been written with the following goals in mind:

1.1.6.1 To describe staff obligations to satisfying the requirements of the Protection of Personal Information Act (PoPIA);

1.1.6.2 to establish business rules to ensure the integrity, availability and confidentiality of all GWK information;

1.1.6.3 to educate employees about their obligations for the protection of all GWK information; and

1.1.6.4 to be read in conjunction with any existing IT policy as well as the Group's PAIA Manual.

1.2 Status and application of policy

This policy applies to the entire GWK Group and should also be conveyed and applied to all contractors, suppliers and other persons acting on behalf of GWK Group.

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**.

POPIA does not apply in situations where the processing of personal information is conducted in the course of purely personal or household activities, or where the personal information has been de-identified.

All employees are bound to this document as part of the GWK standard terms and conditions of employment.

Where non-employees, such as contractors, are permitted access to GWK' information systems, they shall likewise contractually be required to adhere to the terms of this policy.

1.3 Updates and amendments

Updates to this policy and related information shall from time to time be published on the GWK intranet and website.

Amendments to, or a review of this Policy, will take place on an *ad hoc* basis or at least annually.

1.4 Further Information

Further information about this document can be obtained from the GWK Information Officer, as defined below.

2 PRIVACY

2.1 Statutory appointments

THE GWK GROUP INFORMATION OFFICER is DEREK LINDE whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and POPIA. He is assisted by SELOMé JORDAAN who will function as the Group's Deputy Information Officer.

THIS POLICY has been put in place throughout the GWK Group and training on this policy and POPIA will be conducted by either GWK Group training third party service providers or the Group Compliance function.

2.2 Audit process

Compliance with this policy shall be monitored through internal audit processes established by the information security management forum in consultation with the Legal and IT departments. External audits may be periodically commissioned by the information security management forum.

2.3 Collection of evidence

In the event that an employee suspects that a breach of this policy may have occurred on an information system (whether relating to GWK or client information), no further action is permitted in respect of such information system until such time as the IO has authorised same.

2.4 Information Classification

Information Classification is the process of assigning value to information in order to organize it according to its risk to loss or harm from disclosure.

The classification process is set out in the Data Classification Policy, whilst the handling thereof is set out in the Data Handling Policy.

3. LAWFUL PROCESSING CONDITIONS

The following obligations apply to all GWK staff when collecting, processing or destroying Personal Information. Should any staff member require clarity on any aspect of these requirements, their queries may be directed at either the Information Officer or Deputy Information Officer.

3.1 Accountability

The GWK Information Officer will ensure that the conditions and all the measures set out in POPIA are complied with at the time of determining the purpose and means of the processing.

Accordingly, the Information Officer will ensure the following:
- GWK will identify and appoint resources as required across the organization to fulfil the requirements wherever personal information is processed
- Sufficient budgetary resources are allocated as needed
- The relevant stakeholders are adequately trained to fulfil their obligations
- Awareness programs are provided to ensure that all staff are aware of POPIA and its implications for daily operations
- Privacy risk is determined through assessments, and reported via the existing risk management channels
- The existence, location and use of personal information is recorded and monitored
- Data subject requests are recorded and addressed wherever they occur, in line with the PAIA Manual
- Related legislation is integrated into privacy management, including specific consideration of retention periods and monitoring
- GWK registers with the Regulator and remains current with published regulations as these occur
- Third-party contracts adequately account for compliance with POPIA.

3.2 Processing Limitation

Personal information may **only** be processed in a fair and lawful manner and only with the consent of the data subject, unless specifically prescribed by any law.

Staff must ensure the following:

- **Personal information must be obtained directly from the Data Subject. The data subject must be referred to the GWK Privacy Notice PRIOR to providing personal information.**
- **The Data Subject must be aware that you have gathered his/her information and consented to the information being used.**
- **The Data Subject must have consented to information being shared and used by you, if the personal information has been gathered from a third party.**
- **The amount of information being gathered may not be excessive.**
- **Consent to process client information is obtained from clients (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship**
- **Should any third parties request access to personal information processed by GWK, this may only be provided with the approval of the GWK Information Officer. Conversely, when a third party shares personal information they are processing, GWK must ensure that this is with the approval of an authorised individual within their organization.**

3.3 Purpose Specification

Personal information may only be processed for specific, explicitly defined and legitimate reasons.

The staff member must ensure the following:

- **The specific, explicit and lawful purpose for which the personal information is being collected must be documented and adhered to.**
- **The Data Subject must be aware of the purpose for which the data has been collected.**
- **All personal information collected must correspond to legitimate reasons for collecting.**

- **Personal information may only be retained for the time periods specified in GWK's Corporate Retention Policy**.
- **Keep track of when personal information must be destroyed**.
- **Document the process that will be used to destroy Personal Information, in a manner that prevents its reconstruction, after you are no longer authorized to retain such record.**

3.4 Further processing limitation

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

The staff member must ensure the following:

- **The intended reuse of personal information must be in accordance and compatible with the purpose for which it was collected.**
- **The Data Subject must be aware of the continued use of their personal information.**

3.5 Information quality

The responsible party must take reasonably steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary.

- **Ensure that personal information is reliable and accurate at all times.**
- **Data Subjects may update their information or withdraw consent by contacting GWK**.

3.6 Openness

The data subject whose information you are collecting must be aware that you are collecting such personal information and for what purpose the information will be used.

The Operator must ensure the following:

- **Proof of consent for collecting and using personal information from the Data Subject is extremely important. Consent must be explicit, and evidence of consent must be retained. Silence does not equal consent.**
- **The Data Subject must be informed of the purpose for which the information is being gathered at the time the information is being gathered or as soon as practically possible after collection.**
- **Inform the Data Subject who the responsible party is.**
- **Inform the Data Subjects of their right to lodge a complaint with the Information Regulator.**
- **Advise the Data Subject of his/her rights to access his/her information and to object to the processing of said information.**

3.7 Security Safeguards

Personal information must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorized destruction and disclosure.

The Responsible Person must determine and ensure:

- **Identify procedures in collaboration with the IT Department to identify any foreseeable internal and external risks to personal information.**
- **Identify processes to prevent personal information from falling into unauthorized hands.**
- **Determine which employees are permitted access to personal information and what information they are permitted to access.**

- **Identify processes to alert you when personal information is accessed or modified without authorization.**
- **Determine processes to identify the source of a data breach and the procedure to follow to neutralize such breach.**
- **Continually update safeguards in response to new risks or deficiencies in previously implemented safeguards.**
- **Prevent and/or address the reoccurrence of a data breach.**
- **Ensure Non-disclosure agreements, alternatively data protection addendums are in place when sharing personal information with an external operator.**
- **Inform the Data Subject that their personal information has been compromised.**
- **Inform the Information Regulator of any security breach.**

3.8 Data subject participation

Data subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them.

Staff must ensure that Data Subjects are advised as follows:

- **The Data Subject's rights regarding access to information being held by GWK.**
- **The Data Subject's right to correct personal information that GWK holds or withdraw consent to use such information.**

4. SAFEGUARDING PI

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

Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information, the greater the security required.

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

GWK Group will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

Employment contracts contain contractual terms for the use and storage of employee information. Confidentiality clauses are included to reduce the risk of unauthorised disclosures of personal information for which GWK Group is responsible.

GWK Group's operators and third-party service providers enter into service level agreements with GWK Group where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement, alternatively addendums. This is, however, an ongoing process that will be evaluated as needed.

The following procedures are in place in order to protect personal information:

- Every employee, current or new, employed within the GWK Group will be subjected to compliance with this Policy;
- GWK archived client information is stored on site, which is also governed by POPIA, access is limited to these areas to authorized personal.

- All electronic files or data are BACKED UP by the Group IT Division which is also responsible for system security that protects third party access and physical threats. The Group IT Division is responsible for Electronic Information Security;

Documents may also be stored off-site, in storage facilities approved by the Company.

5. DESTRUCTION

Documents may be destroyed after the termination of the retention period specified in GWK's Corporate Policy. Should there be a need to retain information beyond this point for statistical or trend analysis, the personal information must be de-identified prior to this occurring.

Each business unit is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents may be returned to the holder thereof, if so requested.

After completion of the process in above, the Manager of the business unit shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by the relevant business unit.

The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal, if and where applicable.

6. CLEAN DESK POLICY

6.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

6.2 Computer workstations must be locked when workspace is unoccupied.

6.3 Computer workstations must be shut completely down at the end of the workday.

6.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

6.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

6.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

6.7 Laptops must be either locked with a locking cable or locked away in a drawer.

6.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

6.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

6.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

6.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

6.12 Lock away portable computing devices such as laptops and tablets.

6.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

6.14 Office Access:

6.14.1 Physical access to facilities containing sensitive information shall be restricted in a manner directed by the IO.

6.14.2 Entry to the office is by means of fingerprint readers or access tags. Server rooms are access controlled by means of access tags and physical keys. Only a select few have access to the server rooms and should be approved by management.

6.14.3 Should a third party require access to a server room, such third party must be supervised by a member of the GWK IT department (or person nominated by the IT department) for the duration that such third-party access is required.

7. TRANSFER OF PI

7.1 Internally

PI may only be transferred internally amongst GWK employees, subsidiaries and/or third parties if:

- There is a legitimate purpose, for example, Financing handing over a file for collection to Legal; or
- The Data Subject has specifically consented to the transfer, for example, Financing transferring personal information to Insurance; or
- The third party has signed a non-disclosure agreement to protect personal data and/or the Data Subject has consented thereto.

7.2 Transborder

The transfer of personal information to a foreign country is prohibited, if the foreign country does not have adequate protection of personal information in place. The possibility exists that the personal information (information knowing no borders) may be processed in a manner that violates the Data Subject's right to privacy, including the right to determine the use of his or her personal information.

It is a feature of data protection legislation globally that unless the equivalent protection is provided in the foreign country, the transfer of the personal information to that country is prohibited, alternatively allowed subject to the fulfilment of conditions aimed to promote the protection of the personal information, regardless of the fact that there may be insufficient or inadequate laws in doing so in the foreign country.

8. ACCEPTABLE USE OF ASSETS

8.1 Company property

Electronic communication systems and all messages generated on or handled by an employee is considered to be the property of GWK.

8.2 No expectation of privacy

The IT department automatically monitors the use of the electronic communication systems and may be required to review the contents of stored or transmitted data in the course of their duties. Such actions shall at all times be within the ambit of existing GWK policies.

8.3 Encryption of electronic communications and devices

8.3.1 Employees should note that most electronic communications are by default not secure.

8.3.2 In certain instances, this policy prescribes the use of encryption technologies.

8.3.3 Electronic communications may only be encrypted utilising technologies approved by the IT Department and further subject to any conditions imposed in respect thereof in terms of procedures.

8.4 Acceptable and unacceptable use

8.4.1 Employees must comply with the Company's Acceptable Use Policy in place from time to time (forming part of the HR policy).

8.4.2 Employees are to comply with all IT related policies.

9. DIRECT MARKETING

There is no restriction on direct marketing by electronic communication to existing customers, provided that the customer is afforded the opportunity of opting out of further communications with the responsible party.

Where the Data Subject is not a customer, consent to the processing of personal information for the purposes of direct marketing (opt in) is required. The responsible party must approach the data subject for consent to direct marketing in electronic communications unless such consent has previously been withheld. If the person approached does not expressly agree to receipt of further electronic communications (opt in), any further communications to that person will be unlawful.

10. VIOLATION

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

GWK Group will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, GWK Group will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

GLOSSARY

Definitions, Abbreviations and Acronyms

TERM	DEFINITION
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.
Child	means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.
Competent Person	means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

Confidential Information	any information, including Personal Information, in any format or material embodiment which is by its nature confidential and includes technical, commercial or financial information, know-how, trade secrets, employee training programs and/or plans, processes, formulae, hypertext documents or language, programmes, algorithms, machinery, designs, drawings, plans, research, products, financial results and projections, business plans, ideas, account numbers software source code, inventions, business, financial and marketing objectives or strategies, technical specifications and data in whatever form, proprietary intellectual property and the like and includes the fact and extent of the owner's interest in same; client lists or prospective client lists and client details, including names, cell phone numbers and banking details; descriptions of corporate structure, shareholdings, franchise and licensing arrangements; any written information which is labelled "confidential" or "proprietary" before it is disclosed, belonging to or relating to the party disclosing such information ("Disclosing Party") which information is communicated to or otherwise acquired by the other Party ("Receiving Party"), during the course of the Parties' interactions, discussions and negotiations with one another, whether such information is formally designated as confidential or not.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data message	includes a data message as defined in section 1 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002); "form(s)" as referred to in these Regulations, means a form referred to in the annexures to these Regulations or any form which is substantially similar to that form.
Data subject	This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the GWK Group with products or other goods.
De-identify	This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.
Direct Marketing	Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: ✦ Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or ✦ Requesting the data subject to make a donation of any kind for any reason.
Disclosing Party	Means the party disclosing personal information.
Divisions	Business units within GWK Limited, which are not subsidiaries of GWK Limited, for example, the GWK Agri Division, which consists of, amongst others, financing, retail, direct inputs and so forth.
ECTA	Electronic Communications and Transactions Act
Electronic communication	Means any text, voice, soundor image message sent over an electronic communications network, which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
Electronic Communications system	Means all systems used by GWK that enable electronic communications, including (without limitation) the Internet, voice mail, electronic mail and facsimiles.

Employee	Means a part- or fulltime employee of GWK, including any contractor with access to GWK' information systems.
FICA	Financial Intelligence Centre Act No. 38 OF 2001, as amended
Filing system	Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
GWK GROUP	All business units/divisions/subsidiaries within GWK Limited.
GWK LIMITED	Griekwaland Wes Korporatief Limited registered in accordance with the Company laws of the Republic of South Africa with registration number: 1997/022252/07.
Information matching programme	means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject
Information officer	The Information Officer is responsible for ensuring the GWK Group's compliance with PoPIA. Where no Information Officer is appointed, the head of the GWK Group will be responsible for performing the Information Officer's duties. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
IO	Information Officer
Natural person	An individual that establishes a business relationship or enters into a single transaction with an accountable institution and includes a trust, partnership or sole proprietor.
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 GWK Group to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.
PAIA	Promotion of Access to Information Act
Person	Means a natural or a juristic person
Personal Information	Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning: ✦ race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; ✦ information relating to the education or the medical, financial, criminal or employment history of the person; ✦ any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; ✦ the biometric information of the person; ✦ the personal opinions, views or preferences of the person;

	✦ correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; ✦ the views or opinions of another individual about the person; ✦ the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person
PI	Personal Information
POPIA	Protection of Personal Information Act, 2013
Private body	means— (a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; (b) a partnership which carries or has carried on any trade, business or profession; (c) or any former or existing juristic person, but excludes a public body
Processing	The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes: ✦ the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; ✦ dissemination by means of transmission, distribution or making available in any other form; or ✦ merging, linking, as well as any restriction, degradation, erasure or destruction of information.
Public body	means— (a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when— (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation
Receiving party	Means the person receiving personal information, for whatever purpose.
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.
Re-identify	In relation to personal information of a data subject, means to resurrect any information that has been de-identified that

	identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.
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, the GWK Group is the responsible party.
Restriction	Means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information
Special Personal Information	Means personal information concerning: (a) The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings
Subsidiary	A legal entity, either wholly or partially owned, by GWK Limited, as defined in the South African Companies Act as amended from time to time.
Unique identifier	Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.