Privacy Policy

Policy	**Privacy Policy - General Processing of Personal Information**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # A

1. Purpose

The purpose of this policy is to establish a compliance framework for The Business to ensure compliance with the Protection of Personal Information Act.

2. Definitions

2.1 "**availability**" means data being accessible and usable upon demand by an authorised entity.

2.2 **"confidentiality"** means information is not made available or disclosed to unauthorised individuals, entities, or processes.

2.3 **"data"** means the representation of facts as text, numbers, graphics, images, sound, or video and includes all electronic and non-electronic data, either in structured or unstructured form which exists within The Business irrespective of the means of storage or retrieval.

2.4 **"data subject"** means the person to whom personal information relates.

2.5 **"direct marketing"** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

a. promoting or offering to supply, in the ordinary course of business, any goods or service to the data subject; or
b. requesting the data subject to make a donation of any kind for any reason.

2.6 **"electronic communication"** means any text, voice, sound or 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.

2.7 **"filing system"** means any structured set of personal information, whether centralised, decentralised dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.8 **"information"** means data in the context of one or more of:

a. the business meaning of data and related elements;
b. the format in which data is presented;
c. the timeframe represented by the data; and / or
d. the relevance of the data to a given usage.

2.9 **"Information Officer"** of, or in relation to,–

a. a public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of PAIA; or
b. a private body means the head of a private body as contemplated in Section 1 of PAIA; and
c. The Business means the person duly nominated and authorised by The Business management, from time to time, to act as the Information Officer and who is duly registered with the Information Regulator.

2.10 **"integrity"** means protecting the accuracy and completeness of assets.

2.11 **"interruptions"** means an event that causes a disruption, temporary halt or break in an activity of process, to any IT system, infrastructure or application that includes servers, network infrastructure, application such as emails etc., desktops, laptops, or tablets due to physical or system errors, loss of equipment or connectivity, and human error.

2.12 **"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.

2.13 **"person"** means a natural person or a juristic person.

2.14 **"personal information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

a. 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;
b. information relating to the education or the medical, financial, criminal or employment history of the person;
c. any identifying number, symbol, e-mail address, telephone number, location information, online identifier, or other particular assignment to the person;
d. the biometric information of the person;
e. the personal opinions, views, or preferences of the person;
f. correspondence sent by the person that would reveal the contents of the original correspondence;

g. the views or opinions of another individual about the person; and
h. 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.

2.15 **"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; or
c. any former or existing juristic person but excludes a Public Body.

2.16 **"processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

a. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
b. dissemination by means of transmission, distribution or making available in any other form; or
c. merging, linking, as well as restriction, degradation, erasure, or destruction of information.

2.17 **"Promotion of Access to Information Act"** and/or **"PAIA"** means the Promotion of Access to Information Act 02 of 2000.

2.18 **"Protection of Personal Information Act"** and/or **"POPIA"** means the Protection of Personal Information Act 04 of 2013.

2.19 **"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.

2.20 **"public record"** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

2.21 **"record"** means any recorded information regardless of form or medium, including any of the following:

a. writing on any material;
b. 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 divided from information so produced, recorded or stored;

c. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
d. book, map, plan, graph, or drawing;
e. photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;
f. in the possession or under the control of a responsible party; and
g. regardless of when it came into existence.

2.22 **"responsible party"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

2.23 **"special personal information"** means personal information as referred to in Section 26 of POPIA.

2.24 **"the business", "we", "us"** and/or **"The Business"** means The Business, a private body operating as a *company duly registered in terms of the Companies Act 71 of 2008* OR *close corporation duly registered in terms of the Close Corporations Act 69 of 1984* OR *a trust duly lodged and registered with the Master of the High Court as required by the Trust Property Control Act 57 of 1988* OR *sole proprietor trading under the name and style of The Business* OR
*partnership trading under the name and style of The Business *. *Delete option not applicable and insert information regarding the Group if this policy appliesto a Group of Companies.*

3. Policy Statement

3.1 The Business recognises its accountability in terms of the POPIA and its regulations, to all its stakeholders. The Business needs to collect personal information from its employees, clients, suppliers, operators as well as other stakeholders to carry out its business.

To maintain a trust relationship with our stakeholders, we are committed to complying with both the spirit and the letter of POPIA and to act with due skill, care, and diligence when dealing with personal information. This is to mitigate the risk, which may include loss of reputation, fines, imprisonment, and to prevent a significant loss of clients.

The responsibility to facilitate compliance throughout The Business has been delegated to the appointed Information Officer and the Deputy Information Officers *Delete if not applicable*. who have the responsibility of supervising, managing, and overseeing the compliance with POPIA. However, it must be emphasised that the primary responsibility for complying with POPIA lies with all members of staff dealing with personal information. All staff must therefore understand their responsibility in terms of POPIA as well as with this Privacy Policy, the supplementary policies and/or any guidance notes and ensure that they are applied when processing personal information.

This Privacy Policy sets out the approach to managing the compliance risks faced by The Business.

Any breach of this Privacy Policy is considered serious and will result in disciplinary action that could ultimately lead to the dismissal of the offender.

3.2 Breach of this policy and reporting lines
(The following clauses should be amended according to the Company's reporting lines)

3.2.1 Any Employee who is part of, or becomes aware of, a data breach must report to their respective Department Manager / Deputy Information Officer / Information Officer; *Delete option not applicable*

3.2.2 The Department Manager reports to the Deputy Information Officer; *Delete if not applicable*.

3.2.3 The Deputy Information Officer reports to the Information Officer; *Delete if not applicable*.

3.2.4 The Information Officer reports to the Directors / members / partners / trustees / owner of The Business, who in return reports to the InformationRegulator.

3.3 Roles and responsibilities
(The following clauses should be amended according to the company's management structure)

3.3.1 The Information Officer must ensure this policy is followed by each employee through the support of all management levels who must discharge their responsibilities.

3.3.2 The Information Officer and the *Deputy Information Officer* (Delete if not applicable), in their duty to ensure data privacy risk management, must:

a. ensure the implementation of this policy in all business areas;
b. ensure that standard operating procedures are developed for all departments of the business;
c. monitor whether this policy is implemented in all departments of the business.
d. respond to data subject requests and objections subject to paragraph 3.2 above.
e. respond to requests from the Information Regulator and work with the Information Regulator subject to paragraph 3.2 above.

3.3.3 The Information Officer and *Deputy Information Officer*, supported by the IT Department / IT Service Provider (Delete if not applicable), must:
a. Developing IT policies, procedures, standards, and guidelines;
b. Provide technical support;
c. Support the implementation of this policy through appropriate technology investments which comply with this policy;

4. Compliance principles

A. The Information Officer must ensure that the business adheres to the following conditions for the lawful processing of personal information in terms of POPIA

4.1 Condition 1: Accountability

The business must ensure that the conditions of lawful processing of personal information and all measures that give effect to such conditions are complied with at all times.

4.2 Condition 2: Processing limitation

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

4.2.2 Personal information may only be processed providing the purpose for which it is processed, it is adequate, relevant, and not excessive;

4.2.3 You may only process and access information as is allowed for in order to perform your duties in terms of your employment function.

4.2.4 Information may not be accessed, stored, or distributed other than is required by your employment function.

4.2.5 You may only process personal in following legal or contractual obligations, to achieve business goals, alternatively with the consent of the data subject after the purpose has been explained to the data subject, who confirmed that the purpose is understood. You may also process information when the processing is in the legitimate interest of the data subject, the business or a third party.

4.2.6 Information must be collected directly from the data subject where possible. If personal information is collected from another source, the data subject must be advised thereof, and the purpose for the collection.

4.3 Condition 3: Purpose specification

4.3.1 The business may only collect personal information for a specific, explicitly defined, and lawful purpose that relates to the function or activity of the business.

4.3.2 It is the employees' instruction to ensure the data subject is made aware of the purpose for which their personal information is processed.

4.3.3 Each employee may only destroy and/or de-identify personal information as is allowed for by this policy, as well as the Data Destruction Policy and the Data Retention Policy.

4.4 Condition 4: Further processing limits

4.4.1 If information is processed for any other purpose other than the reason why the information was originally collected, then permission for such further processing must be granted by the Information Officer in writing if the further processing is allowed in terms of POPIA.

4.4.2 To assess whether further processing is compatible with the purpose of collection, the business must take account of –

d. The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
e. The nature of the information concerned;
f. The consequences for the data subject's intended further processing of his, her or its personal information;
g. The manner in which the personal information has been collected from the data subject; and
h. Any contractual rights and obligations bestowed on the parties.

4.5 Condition 5: Information quality

4.5.1 Information must be kept complete, accurate, must not be misleading, and must be updated where necessary.

4.5.2 If you become aware that a data subject's details have changed, notice must be sent to **thegrowingpatchschool@gmail.com** and the relevant department must be informed of the changes. Changes may only be effected upon proper verification. *Add The Business procedure, if applicable*

4.6 Condition 6: Openness

When The Business collects personal information, reasonable, practicable steps must be taken to ensure that the data subject is aware that the personal information is being collected in line with this and other related policies.

4.7 Condition 7: Security safeguards

4.7.1 Each employee of The Business must secure the integrity and confidentiality of all personal information this is in its or under its control to prevent –

a. The loss of, damage to, or unauthorised destruction of personal information; and
b. The unlawful access to or processing of personal information.

4.7.2 When sharing personal information with an operator, the employee must ensure that a Data Processing Agreement is entered into with the operator that must make provision for the following:

a. the operator must have sufficient security measures in place;
b. the operator must notify The Business immediately of anysuspected security compromise;
c. internal responsibility for information security management;

d. devoting adequate personnel resources to information security;
e. carrying out verification checks on permanent staff who will have access to the personal information;
f. requiring employees, vendors, and others with access to personal information to enter into written confidentiality agreements, and
g. conduct training to make employees and others with access to personal information aware of information security risks presented by the processing.

4.8 Condition 8: Data subject participation

When a data subject provides sufficient proof of identity (for example copy of an identity document or driver's license) the data subject is entitled to:

4.8.1 confirmation whether the company holds information of the data subject;
4.8.2 access to that information;
4.8.3 be advised of his/her/it's right to request the correction or deletion of personal information;
4.8.4 confirmation of what action was taken in response to their request.

4.9 To comply with these principles, you must consider the following policies, procedure, and management tools:

- Internal Privacy Notice;
- Privacy Notice;
- Data Mapping;
- PAIA Manual;
- Personal Information Impact Assessment;
- Standard Operating Procedures;
- Assessment;
- Data Processing Agreements;
- Information Security Policy and supplementary policies;
- Incident Response Policy;
- Clean Desk Policy;
- Data Retention Policy;
- Data Destruction Policy.

B. The business must adhere to the following provisions of POPIA when processing special personal information

4.10 Prohibition on the processing of personal information:

4.10.1 The business will not process 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; unless such processing is justified as follows:

- the Data Subject has consented to process it (in circumstances where we are legally obliged to obtain the data subject's consent); or
- it is necessary to exercise or defend a right or obligation in law; or
- it is necessary to comply with an international legal obligation of public interest; or
- it is for historical, research, or statistical purposes that would not adversely affect your privacy; or
- the data subject deliberately made their personal information public.

C. The business must adhere to the following provisions of POPIA when processing personal information of children

4.11 Prohibition on processing personal information of children:

4.11.1 Definitions:

a. **"child"** means a natural person under the age of 18 years who is not legally competent to take any action or make any decision in respect of any matter concerning him- of herself, without the assistance of a competent person.
b. "**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.

4.11.2 It is important to note that the business may not process personal information concerning a child, unless such processing is:

a. carried out with the prior consent of a competent person;
b. necessary for the establishment, exercise, or defence of a right or obligation in law;
c. necessary to comply with an obligation of international public law;
d. for historical, statistical, or research purposes to the extent that –

i. the purpose serves a public interest, and the processing is necessary for the purpose concerned; or
ii. it appears to be impossible or would involve a disproportionate effort to ask for consent; and
iii. sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

e. of personal information which has deliberately been made public by the child with the consent of a competent person.

D. The business must adhere to the following provisions of the POPIA when marketing directly to a data subject through unsolicited electronic communication

4.12 Prohibition on direct marketing by means of unsolicited electronic communication:

4.12.1 The processing of personal information of a data subject for the purpose of direct marketing through any form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or email is prohibited unless the data subject –

a. has given his, her or its consent to the processing; or
b. is a customer of the business.

4.12.2 In the above context "automatic calling machine" means a machine that is able to do automated calls without human intervention.

4.12.3 The business may approach a data subject only once to request the consent of that data subject and only if the data subject has not previously withheld such consent.

4.12.4 The data subject's consent must be requested in the prescribed manner and form 4 to the Regulations.

4.12.5 The business may only process the personal information of a data subject who is a customer of the business if –

a. the business has obtained the contact details of the data subject in the context of the sale of a product or service;
b. the purpose of direct marketing is through the business's own similar products or services; and
c. the data subject has been given a reasonable opportunity to object, free of charge, and in a manner free of unnecessary formality, to such use of his, her, or its electronic details –

i. at the time when the information was collected; and
ii. on the occasion of each communication with the data subject for the purpose of direct marketing if the data subject has not initially refused such use.

4.12.5 Any communication for the purpose of direct marketing must contain –

a. details of the identity of the sender or the person on whose behalf the communication has been sent; and
b. an address or other contact details to which the recipient may send a request that such communications cease.

E. The business must adhere to the following provisions of POPIA when transferring personal information outside of the Republic of South Africa

4.13 The business may not transfer personal information about a data subject to a third party who is in a foreign country unless the personal information that is collected automatically is collected by third parties whose technology we use to provide website functionality and acquire website analytics information. Some of these third parties will be outside of the borders of South Africa and data subject's information will be stored outside the borders of South Africa. We make use of productivity software solutions such as Microsoft 365 or Google Business and the information collected through this third party will be kept on the servers used by of the software solution provider. *Amend if applicable*

5. Training

Staff will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the policies and procedures, or IT Infrastructure.

Training may be provided through information sessions, regular emails to all staff as well as pre-recorded online webinars, and will cover the latest subjects related to the use of The Business IT systems and applications, the applicable laws relating to data protection, and The Business's data protection, and related policies and procedures. Completion of training is compulsory.

If you have any questions or concerns about anything in this policy, do not hesitate to send your query to _____.

6. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals may be subject to loss of the business's information resources access privileges and/or further civil and criminal prosecution.

7. Document control

Creation date	
Division name	The Business Management
Author name	
Author position	
Last updated	
This version	
Latest version approved by Board of Directors / Members / partners / trustees / owner of The Business	

8. Change history

Date	Author	Version	Change reference

9. Policy approval

Signed: _____

Date: _____