PROTECTION OF PERSONAL INFORMATION ACT, 4 of 2013 ("POPIA")

Details of the School:

Postal address of the School:	PO Box 1455 Hammanskraal 0400
Street address of the School:	Portion 4, Farm Klipdrift 116, Hammanskraal / 1 Eike Street, Hammanskraal. 0040
Telephone number of the School:	012 711 8600
E-mail Address of the School	admin@prestigecol.co.za
Information Officer at the inception of Policy: Contact in writing:	Janos Pentz popi@prestigecol.co.za Registration Number:22009/2021-2022/IRRTT
Deputy Information Officer at the inception of Policy Contact in writing:	Lezelle Strydom popi@prestigecol.co.za Registration Number:22009/2021-2022/IRRTT

1. INTRODUCTION

1.1 Prestige College (herein after "Company") is a non-profit company with registration number 1994/09429/08.

1.2 The Company is obligated to comply with The Protection of Personal Information Act, 2013 (Act No 4 of 2013) (herein after "POPIA").

1.3 The POPIA requires the Company to inform the Data Subject as provided for in Section 1 of the POPIA, as to the way their personal information will be used, protected, disclosed, and destroyed.

1.4 This Policy sets out the way the Company deals with the Data Subject's personal information and stipulates the purpose for which said information is used.

1.5 The POPIA was enacted to give effect to the·constitutional right to privacy by safeguarding personal information when processed by 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.

1.6 The POPIA assigned an obligation on the protection of the personal information which intends to balance, through justifiable limitations, the following three competing interests, namely:

- The constitutional right to privacy (which requires personal information to be protected) against other rights, particularly the right of access to information;
- protecting important interests, including the free flow of information within the Republic and across international borders; and
- the needs of society to have access to and to use personal information for legitimate purposes, for example, to enable the Company to render services

1.7 The Act furthermore introduced and prescribed the minimum threshold requirements for the lawful processing of personal information by a private or public body.

1.8 The Management of Prestige College is committed to:

- To safeguard the personal information held by the school from threats, whether internally or externally, deliberate or accidental and thus protecting the right of privacy of all Data Subjects.
- Protecting the School's records and information in order to ensure the continuation of the day to day running of the school.
- Regulating the manner in which personal information is processed by the school and stipulating the purpose for which information collected is used.
- Appointing Information Officers to ensure respect for and to promote, enforce and fulfil the rights of Data Subjects.
- To protect the School from the compliance risks associated with the protection of personal information which includes:
  a) breaches of confidentiality where the School could suffer a loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately;
  b) failing to offer a choice, including the choice where all data subjects should be free to decide how and for what purpose the School may use information relating to them; and
  c) any instances of any reputational damage where the School could suffer a decline in its reputation or its good name is impugned through the actions of another party who disseminates or has gained unauthorised access to any personal information of the school's data subjects.

2. PURPOSE OF POLICY

The purpose of this policy is to inform the Data Subject and enable the Company to comply with:

- The laws in respect of personal information that the Company holds in respect of Data Subjects.
- Follow good practice;
- Protect the Company's reputation;
- Protect the Company from the consequences of a breach of its responsibilities; and

- Protect the Data Subject against loss or breach of their personal information.

3. BACKGROUND AND SCOPE

3.1 The purpose of POPIA is to regulate the processing, storage and dissemination of personal information by public and private bodies so as to ensure the right of the Data Subject to the privacy of their Personal Information. This policy applies to information relating to identifiable Data Subjects in terms of POPIA.

3.2 Personal information may only be processed if the process meets the conditions of the Act. There are eight distinct conditions that need to be met to be acting lawfully:

a. Accountability
b. Processing limitation
c. Purpose specification
d. Use limitation
e. Information quality
f. Openness
g. Security safeguards
h. Individual/data subject participation

3.3 The Policy applies to all employees, directors, sub-contractors, agents and appointees of the Company. The provisions of the Policy are applicable to both on and off-site processing of personal information.

4. POLICY STATEMENT

The Company collects and uses Personal Information of employees, individuals and· corporate entities with whom it works, in order to operate and carry out its business effectively. The Company regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery

and essential to maintaining confidence between the Company and its stakeholders. The Company therefore fully endorses and adheres to the principles of POPIA.

5. DEFINITIONS

The following definitions in the POPIA are key in determining what activities are undertaken by education institutions will be affected by the Policy:

Board of Directors	Means the body of people authorised by the School's constitutional documents to jointly supervise and govern the School, including but not limited to the board of directors, trustees or governors;
Company	Means Prestige College NPC, as duly registered in terms of the provisions of the Companies Act, 2008 (Act No. 71 of 2008);
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 Data
Consent	This means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Protection Laws	means any data protection or data privacy laws relating to Personal Information, applicable to the activities of the company, including POPIA, any laws, regulations, guidelines and/or codes of conducts issued by the Information Regulator.

Data Subject	This refers to the natural or juristic person to whom the personal information relates, such as individual pupils, parents, employees or a company that supplies the school with services, products or other goods.
De-Identify	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.
Filing System	This 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.
Identifier	This 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.
Information Officer	The Information Officer is responsible for ensuring the organisation's compliance with POPIA but it is ultimately the Head of the school who is responsible for ensuring that the Information Officer's duties are performed. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties.
Information Regulator	means the Information Regulator appointed in terms of POPIA.
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 organisation and whose service requires access to the personal information of pupils, parents and employees. (When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.)
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 assignments 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; or ● 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. Categories of Data Subjects and their Personal Information: ● Natural Persons: Names; contact details; physical and postal addresses; date of Birth; ID number; tax-related information; nationality; gender; confidential correspondence.

	● Juristic Person/Entities: Names of contact persons; the name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax-related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; B-BBEE information ● Contracted Service Providers: Names of contact persons; the name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax-related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; B-BBEE information ● Directors: Gender; marital status; colour; race; age; language; education information; financial information; employment history; ID numbers; physical and postal address; contact details; opinions; criminal record; well-being
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.
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.
Record	Means any recorded information, regardless of form or medium, including: ● writing on any material;

	● information produced, recorded or stored by means of any recording equipment, computer equipment, whether hardware or software or both, or other devices, 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; or ● photograph, film, negative, tape or other devices 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. o in the possession or under the control of a responsible party; o whether or not it was created by a responsible party and o regardless of when it came into existence.
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 Party	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. The school is the responsible party.
Security Event	means where there is reason to believe or to suspect that Personal Information has been acquired, disclosed, used, dealt with in any way whatsoever · or accessed by an unauthorised party or is reasonably likely to be acquired, disclosed, used or accessed by an unauthorised party.

Service Providers	means a service provider of the Company appointed by the Board of Directors for the purposes of POPIA known as an Operator, who processes Personal Information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that responsible party.
Special Personal Information	● the religious, philosophical, or political beliefs of the Data Subject; ● the race or ethnic origin of the Data Subject; ● trade union membership of a Data Subject; ● the health of a Data Subject; ● biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs) of a Data Subject; and ● criminal behaviour and records of a Data Subject.

6. PROCESSING PERSONAL INFORMATION

6.1 Purpose of Processing

The Company uses the Personal Information under its care in the following ways:

- Administration of agreements;
- Detecting and prevention of fraud, crime, money (laundering and other malpractice;
- Marketing, boarding, leases and sales;
- In connection with legal proceedings;
- Administration and legislation compliance;
- Keeping of accounts and records; and
- Complying with legal and regulatory requirements.

6.2 Categories of Data Subjects and their Personal Information:

Entity Type	Personal Information Processed
Parents	Names; contact details; physical and postal addresses; date of birth; ID number; tax-related information; nationality; gender; confidential correspondence, Financial Information, Marital Status, CCTV Footage, Credit Records
Learners	Learner Contact Details, Race, Ethnicity, Religion, Unabridged Birth Certificate/ID over 16, Age, Health Information, Personal Circumstances and history, Study Permit (if applicable), Passport Document (if applicable), academic History, Academic Results, Discipline Record, Communication to parents or relating to the child, Extramural activities, Covid information, CCTV footage, Class registers and attendance, Home language, Photos
Employees	Proof of Qualifications, Proof of ID, Proof of Drivers License and PDP, Proof of SACE, Physical and Postal Address, Personal Cell Phone Number for WhatsApp and other communication, School Email address and communication Records, "Financial details: Tax number; tax directives, bank details", Remuneration, bonuses, increases, Credit checks, Next of kin, marital status, pension details, CCTV surveillance footage / searches of person and property, Performance records, Discipline, grievance records, Leave records, travel records, Photos / videos, Training records / Skills development, Religion (when relevant to organisational nature / job), Breathalyser or Similar Tests,Termination records, dismissal, resignation, retirement, separation agreements, exit interviews, etc., Pension, final payments, settlements, Death records / disability boarding / correspondence, UIF, certificate of service, tax directives, Post-termination records, CCMA referrals / litigation records, References; forwarding contact details

Juristic Persons/ Entities	Names of contact persons; the name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax-related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; B-BBEE information
Contracted Service Providers	Names of contact persons; the name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax-related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Directors	Gender; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being

6.3 Categories of recipients for processing of Personal Information

6.3.1 The Company may supply the Personal Information to any party to whom the Company may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Conducting due diligence checks; and
- Accounting services.

6.3.2 Furthermore, the Company may supply Personal Information to anybody enacted in terms of the laws of the Republic of South Africa and in terms of which laws the Company is obligated to share such information, which may include but is not limited to the South African Revenue Service, Department of Public Works, Department of Employment and Labour.

6.3.3 Actual or Planned Transborder Flows of Personal Information

Personal Information may be transmitted transborder to the Company's authorised service providers or suppliers in other countries, and Personal

Information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws. The Company will endeavour to ensure that its service providers or suppliers will make all reasonable efforts to secure said data and Personal Information.

6.3.4 Retention of Personal Information Records

The Company may retain Personal Information records indefinitely unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information, the Company shall retain the Personal Information records to the extent permitted or required by law.

6.3.5 General Description of Information Security Measures

The Company employs technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:
Firewalls;
Virus protection software and update protocols; Logical and physical access control; and
Secure setup of hardware and software making up the Information Technology infrastructure.

7. ACCESS TO PERSONAL INFORMATION

7.1 All individuals and entities may request access, amendment, or deletion of their own Personal Information held by the Company, subject to relevant legislation. Any requests should be directed, on the prescribed form, to the Information Officer or his/her Deputy Information Officer (The prescribed form, as per Government Gazette 42110 of 14 December 2018 is attached hereto as Annexure A).

7.2 Remedies available if the request for access to Personal Information is refused

7.2.1 Internal Remedies

If the requester would like to appeal the Information Officers decision on requesting personal information, he/she may send an email to the Executive

Principal for review at admin@prestigecol.co.za. The decision taken here will be final. If the request then is refused again and he or she is still not satisfied, then only may the requesters exercise external remedies at their disposal.

7.2.2 External Remedies

A requester that is dissatisfied with the internal remedies at their disposal to disclose information, may lodge a complaint with the Information Regulator in terms of Chapter 10 of POPIA.

7.2.3 Grounds for Refusal

The Company may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which the Company may refuse access include inter alia:

(i) Protecting personal information that the Company holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
(ii) Protecting commercial information that the Company holds about a third party or the Company (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third party);
(iii) If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
(iv) If disclosure of the record would endanger the life or physical safety of an individual;
(v) If disclosure of the record would prejudice or impair the security of property or means of transport;
(vi) If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
(vii) If disclosure of the record would prejudice or impair the protection of the safety of the public;
(viii) The record is privileged from production in legal proceedings unless the legal privilege has been waived;

(ix) Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of the Company;

(x) Disclosure of the record would put the Company at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;

(xi) The record is a computer programme; and

(xii) The record contains information about research being carried out or about to be carried out on behalf of a third party or the Company.

7.2.4 Records that cannot be found or do not exist

If the Company has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

8. DUTIES AND RESPONSIBILITIES

8.1 Information Officer (and/or Deputy Information Officer/s)

The school's Information Officer (or delegated Deputy Information Officer/s) is responsible for:

- keeping the Management Team and/or Board of Governors and/or Board of Trustees of the School updated about the School's responsibilities under POPIA;
- continually analysing POPIA regulations and/or notices issued by the Information Regulator in order to align these with this Policy and procedures thereto;
- ensuring that POPIA Audits are scheduled and conducted on a yearly basis;;
- ensuring that the School has accessible processes in place makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the School;
- approving any contracts entered into with operators, employees and other

third parties which may have an impact on the Personal Information held by the School;

- oversee the amendment of the School's employment contracts and other service level agreements;
- ensure that employees and other persons acting on behalf of the School are fully aware of the risks associated with the processing of personal information and that they remain informed about the School's security controls.
- organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the School
- addressing employees' POPIA related questions;
- addressing all POPIA related requests and complaints; and
- working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

8.2 IT Administrator

The school's IT Administrator is responsible for:

- ensuring that the school's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards;
- ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services;
- ensuring that servers containing personal information are sited in a secure location, away from the general office space;
- ensuring that all electronically stored personal information is backed-up and tested on a regular basis;
- ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts;
- ensuring that personal information being transferred electronically is

encrypted;

- ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software;
- performing regular IT audits to ensure that the security of the school's hardware and software systems are functioning properly;
- performing regular IT audits to verify whether the electronically stored personal information has been accessed or acquired by any unauthorised persons; and
- performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the school's behalf. For instance, cloud computing services.

8.3 The school's Marketing Team is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the school's websites, including those attached to communications such as emails and electronic newsletters;
- addressing any personal information protection queries from journalists or media outlets such as newspapers; and
- where necessary, working with persons acting on behalf of the school to ensure that any outsourced marketing initiatives comply with POPIA.

8.4 Employees and other persons acting on behalf of the School

Employees and other persons acting on behalf of the school will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain pupils, parents, suppliers and other employees. Employees and other persons acting on behalf of the school are required to treat personal information as a confidential business asset and to respect the privacy of Data Subjects in the following manner:

- employees and other persons acting on behalf of the school may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the school 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 the school 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 the school will only process Personal Information where:
    - the data subject, or a competent person where the data subject is a child, consents to the processing; or
    - the processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party; or
    - the processing complies with an obligation imposed by law on the responsible party; or
    - the processing protects a legitimate interest of the Data Subject; or
    - the processing is necessary for pursuing the legitimate interests of the School or of a third party to whom the information is supplied.

Employees and other persons acting on behalf of the School 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

media such as external drives, CDs or DVDs 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. For instance, in a locked drawer of a filing cabinet;
- ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer;
- taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the parent or customer phones or communicates via email;
- 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. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner;
- undergoing POPIA Awareness training from time to time; and
- reporting any suspicious activity, security breach, interference, modification, destruction or the unsanctioned disclosure of personal information, immediately to the Information Officer.

Employees and other persons acting on behalf of the school will under no circumstances:

- process or have access to Personal Information where such processing or access is not a requirement to perform their respective work-related tasks or duties;
- save copies of Personal Information directly to their own private computers, laptops or other mobile devices like tablets or smartphones. All personal information must be accessed and updated from the school's administrative

system and central database on dedicated servers;

- share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure; or
- transfer personal information outside of South Africa without express permission from the Information Officer.

8.5 Training and Dissemination of Information

- This Policy has been discussed throughout Prestige College.
- Training on the Policy and POPIA have taken place with all affected persons.
- Updated training will take place on a regular basis.
- Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of the members of Prestige College.

9. EIGHT PROCESSING CONDITIONS

POPIA is implemented by abiding by eight processing conditions. The Company shall abide by these principles in all its possessing activities.

9.1 Accountability

The School must assign and register the Information Officer and Deputy Information Officers who will ensure that personal information is collected and processed in accordance with POPIA. These persons will oversee and manage the School's compliance with POPIA and will furthermore handle all requests made by learners, parents, staff and all relevant stakeholders, for access to information.

The designated persons will ensure that the School takes 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 responsibilities outlined in this policy.

9.2 Processing Limitation

Personal information must only be collected for a specific, explicitly defined, and lawful purpose or any other legitimate purpose.

9.2.1 Lawful grounds

(a) The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant, and not excessive. The Company may only process Personal Information if one of the following grounds of lawful processing exists:

(i) The Data Subject consents to the processing (Privacy and Informed Consent Form as per annexure "B");

(ii) Processing is necessary for the conclusion or performance of a contract with the Data Subject;

(iii) Processing complies with a legal responsibility imposed on the Company;

(iv) Processing protects a legitimate interest of the Data Subject;

(v) Processing is necessary for the pursuance of a legitimate interest of the Company, or a third party to whom the information is supplied.

(b) The Company may only process Special Personal Information under the following circumstances:

(i) The Data Subject has consented to such processing; The Special · Personal Information was deliberately made public by the Data Subject;

(ii) Processing is necessary for the establishment of a right or defence in law;

(iii) Processing is for historical, statistical, or research reasons; and

(iv) If the processing of race or ethnic origin is to comply with employment equity laws.

(c) All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may

object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the data subject withdraws consent or objects to the processing, then the Company shall forthwith refrain from processing the Personal Information.

9.2.2 Collection directly from the Data Subject

Personal Information must be collected directly from the Data Subject, unless:

(a) Personal Information is contained in a public record;

(b) Personal Information has been deliberately made public by the Data Subject;

(c) Personal Information is collected from another source with the Data Subject's consent;

(d) Collection of Personal Information from another source would not prejudice the Data Subject;

(e) Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;

(f) Collection from the Data Subject would prejudice the lawful purpose of the collection; and

(g) Collection from the Data Subject is not reasonably practicable.

9.3 Purpose Specification

The Company shall only process Personal Information for the specific purposes as set out and defined in paragraph 5.1. (supra). Any further processing of personal information (for a secondary purpose) by the School, must be upon the consent obtained from the relative Data Subject.

9.4 Further Processing

New processing activities must be compatible with the original purpose of

processing. Further processing will be regarded as compatible with the purpose of collection if:

(a) Data Subject has consented to the further processing;

(b) Personal Information is contained in a public record;

(c) Personal Information has been deliberately made public by the Data Subject;

(d) Further processing is necessary to maintain, comply with or exercise any law or legal right; or

(e) Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party

9.5 Information Quality

9.5.1 The Company shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. The Company shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

9.5.2 The Company should as far as reasonably and practicably possible implement the following guidelines when collecting Personal Information:

(a) Personal Information should be dated when received;

(b) A record should be kept of where the Personal Information was obtained;

(c) Changed to information records should be dated;

(d) Irrelevant or unneeded Personal Information should be deleted or destroyed; and

(e) Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

9.6 Openness

9.6.1 The Company shall take reasonable steps to ensure that the Data Subject is made aware of:

(a) What Personal Information is collected, and the source of the information;

(b) The purpose of collection and processing;

(c) Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;

(d) Whether the collection is in terms of any law requiring such collection;

(e) Whether the Personal Information shall be shared with any third party; and

(f) If such Personal Information is to be shared with a third party, obtain the Data Subject's consent to share such Personal Information, save for instances where the Company is legally obliged to share the Personal Information.

9.7 Security Safeguards

9.7.1 The Organisation and its employees must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal information, and against the accidental loss of, or damage to, personal information.

9.7.2 The Organisation will put in place procedures and technologies to maintain the security of all personal information. Personal Information may only be transferred to an operator if the operator has agreed to comply with those procedures and policies or has adequate security measures in place.

9.7.3 Users may refer to the Organisation's information security and related policies for further information concerning the Organisation’s security safeguards.

9.7.4 Security procedures at the Prestige College include, but is not limited to:

- **Written records**
  - Personal Information records should be kept in locked cabinets or safes;
  - When in use Personal Information records should not be left unattended in areas where unauthorised persons may access them;
  - Personal Information which is no longer required should be disposed of by shredding or incineration; and
  - Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

- **Electronic Records**
    - Personal Information records should be kept in locked cabinets or safes;
    - All electronically held Personal Information must be saved in a secure database;
    - As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices;
    - All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently; and
    - Electronic Personal Information which is no longer required must be deleted from the individual laptops or computers and the relevant database.
    - Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall take all necessary steps to remotely delete the information, if possible.

9.8 Data Subject Participation

9.8.1 The Data Subject has the right to request access to amendment, or deletion of their Personal Information. .

9.8.2 All such requests must be submitted in writing to the Information Officer in the prescribed form, Annexure A.

9.8.3 Unless there are grounds for refusal as set out in paragraph 6.2, above, the Company shall disclose the requested Personal Information:

(a) On receipt of adequate proof of identity from the Data Subject, or requester;

(b) Within a reasonable time;

(c) On receipt of the prescribed fee, if any; and

(d) In a reasonable format.

9.8.4 The Company shall not disclose any Personal Information to any party unless

the identity of the requester has been verified.

10. DESTRUCTION OF DOCUMENTS

10.1 Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time.

10.2 The Company is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis and in accordance with this Policy.

10.3 Files must be checked to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

10.4 The physical documents must be destroyed beyond reconstruction.

10.5 Deletion of electronic records must be done in consultation with the external IT contractor, to ensure that deleted information is incapable of being reconstructed and/or recovered.

11. STATUTORY RETENTION PERIODS

Legislation	Document Type	Period
Companies Act	● Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; ● Notice and minutes of all Council Meetings, including resolutions adopted and documents made available to Council Members and Associations;_ ● Copies of reports presented at the annual general meeting of the company; ● Copies of annual financial statements	7 Years

	required by the Act; ● Copies of accounting records as required by the Act; ● Record of directors and ● past directors, after the director has retired or resigned from the company. ● Written communication to Council Representatives; and ● Minutes and resolutions of Board Meetings or any other meetings.	
	● Registration Certificate ● Memorandum of Incorporation and alteration and amendments ● Rules ● Securities register and uncertified securities register; and ● Register of company secretary and auditors.	Indefinitely
Consumer Protection Act	● Full names, physical address, postal address and contact details; ● ID number and registration number; ● Contact details of public officer in case of a juristic person; ● Service rendered; ● Cost to be recovered from the consumer; ● Frequency of accounting to the consumer; ● Amounts, sums, values, charges, fees, remuneration specified in monetary terms; ● Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions.	3 Years
Financial Intelligence Centre Act	● Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the	5 Years

	customer; ● If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; ● If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; ● The manner in which the identity of the persons referred to above was established; ● The nature of that business relationship or transaction; ● In the case of a transaction, the amount involved and the parties to that transaction; ● All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; ● The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; and ● Any document or copy of a document obtained by the accountable institution.	
Tax Administration Act	Section 29 documents which: ● Enable a person to observe the requirements of the Act; ● Are specifically required under a Tax Act by the Commissioner by the public notice; and	5 Years

	• Will enable SARS to be satisfied that the person has observed these requirements.	
Income Tax Act	• Amount of remuneration paid or due by him to the employee; • The amount of employee's tax deducted or withheld from the remuneration paid or due; • The income tax reference number of that employee; • Any further prescribed information; and • Employer Reconciliation Return.	5 Years
Value Added Tax Act	• Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; • Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; • Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; • Documentary proof substantiating the zero rating of supplies; and • Where a tax invoice, c_redit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the	5 Years

	Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	

12. POLICY REVIEW

The Organisation will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required, taking into account changes in the law and organisational or security changes.

Issued by the Information Officer.

J. Pentz
Information Officer

Ms HC Pienaar
Executive Principal

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer below:	
Name	
Email address	

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

Particulars of Data Subject	
Name and Surname	
Identity Number	
Mobile number	
Email address	
Years associated with Prestige College	

Request	
I request Prestige College to:	
	Inform me where the school holds any of my personal information

	Provide me with a record or description of my personal information
	Correct or update my personal information
	Destroy or delete a record of my personal information

Signature	Date

ANNEXURE B: POPI Compliant Form

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act. *Please submit the completed form to the Information Officer below:*	
Name	
Email address	

Where we are unable to resolve your complaint to your satisfaction you have the right to complain to the Information Regulator who can be contacted at http://www.justice.gov.za/inforeg/index.html

Particulars of Complainant	
Name and Surname	
Identity Number	
Mobile number	
Email address	
Years associated with Prestige College	

Details of complaint.

Desired Outcome

Signature	Date

ANNEXURE C: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

"Personal Information" (PI) shall mean the 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 whether the information is recorded electronically or otherwise.

"POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

Prestige College undertakes to process the personal information of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's POPIA Policy and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.

The employee acknowledges that the collection of his/her personal information is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer.

The employee therefore irrevocably and unconditionally agrees:

1. That they are notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
2. That they consent and authorise the employer to undertake the collection, processing and further processing of the employee's PI by the employer for the purposes of securing and further

facilitating the employee's employment with the employer.

3. Without derogating from the generality of the aforestated, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
4. To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
5. To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
6. To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
7. The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
8. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.
9. The employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of parents, pupils, other employees and suppliers. The employee will treat personal information as a confidential school asset and agrees to respect the privacy of parents, pupils, other employees and suppliers and other employees.
10. To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.
11. Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the school community 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 on behalf of the employer.

Name of Employee:	
Signature:	
Date:	

Name of Employer:	
Information Officer:	
Signature:	
Date:	

ANNEXURE D: SERVICE LEVEL AGREEMENT CONFIDENTIALITY CLAUSE

Personal Information" (PI) shall mean the 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 whether the information is recorded electronically or otherwise.

"POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

1. The parties acknowledge that for the purposes of this agreement that the service provider contracted to Prestige College may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which Prestige College is responsible.
2. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is

acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.

3. The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

4. The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.

5. Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

.

Service Provider:	
Representative:	
Signature	
Date	

For and on behalf of Prestige College	
Information Officer:	
Signature	
Date	