HOËRSKOOL
PRETORIA-NOORD

PROTECTION OF PERSONAL INFORMATION POLICY MANUAL AND COMPLIANCE FRAMEWORK

Table of Contents

1. Entity Details

Hoërskool Pretoria-Noord is an independent school providing educational services and governed by the provisions of the South African Schools Act 84 of 1996, as well as its own constitution.

We are based in Pretoria North and the medium of instruction at the school is Afrikaans. The school offers education in grades 8 to 12.

Information Officer Details

Mr CJC Driescher

Address: 122 Berg Ave
Pretoria North
Pretoria
GAUTENG
0182

Tel: +27 12 546 6590
Email: administrasie@pnhs.co.za

Deputy Information Officer

Address: 122 Berg Ave
Pretoria North
Pretoria
GAUTENG
0182

Tel: +27 12 546 6590
Email: administrasie@pnhs.co.za

2. Introduction

We are committed to compliance with The Protection of Personal Information (POPI) Act which requires us to:

1. Sufficiently inform candidates/applicants/work-seekers (data subjects), hereafter referred to as candidates, the purpose for which we will process their personal information;

2. Protect our Information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy and compliance framework establishes measures and standards for the protection and lawful processing of personal information within our organisation and provides principles regarding the right of individuals to privacy and to reasonable safeguarding of their personal information.

The Information Officer, is responsible for:

- Conducting a preliminary assessment;
- The development, implementation and monitoring of this policy and compliance framework;
- Ensuring that this policy is supported by appropriate documentation;
- Ensuring that documentation is relevant and kept up to date;
- Ensuring this policy and subsequent updates are communicated to relevant managers, representatives, staff, and associates, where applicable.

All employees, departments and individuals directly associated with us are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Any Service Provider that provides Information Technology services, including data storage facilities, to our organisation must adhere to the requirements of the POPI Act to ensure Adequate protection of personal information held by them on our behalf. Written confirmation to this effect must be obtained from relevant service providers.

3. Policy Principles

Principle1: Accountability

- We must take reasonable steps to ensure that personal information obtained is stored safely and securely.

Principle 2: Processing Limitation

- We will collect personal information directly from parents, students, employees and other representatives.
- Once in our possession we will only process or release information with their consent, except where we are required to do so by law. In the latter case we will always inform the relevant parties.

Principle 3: Specific Purpose

- We collect personal information from parents and students required by laws or regulations as well as information to enable us to administrate the education of the students and communicate with parents or representatives.
- We collect personal information from employees required by laws or regulations as well as information to enable us to communicate with employees or representatives.

Principle 4: Limitation on Further Processing

- Personal information may not be processed further in a way that is incompatible with the purpose for which the information was collected initially. We collect personal information for administration and communication, and it will only be used for that purpose.

Principle 5: Information Quality

- We are responsible for ensuring that information is complete, up to date and accurate before we use it. This means that it may be necessary to request individuals, from time to time, to update their information and confirm that it is still relevant. If we are unable to reach a individual for this purpose their information will be deleted from our records.

Principle 6: Transparency/Openness

- Where personal information is collected from a source other than directly from a individual (EG Social media, portals) we are responsible for ensuring that the candidate is aware:
    - That their information is being collected;
    - Who is collecting their information by giving them our details;
    - Of the specific reason that we are collecting their information.

Principle 7: Security Safeguards

- We will ensure technical and organisational measures to secure the integrity of personal information, and guard against the risk of loss, damage, or destruction thereof. Personal information must also be protected against any unauthorised or unlawful access or processing. We are committed to ensuring that information is only used for legitimate purposes with consent and only by authorised employees of our entity.

Principle 8: Participation of Individuals

- Students, parents, employees, and representatives are entitled to know particulars of their personal information held by us, as well as the identity of any authorised employees of our entity that had access thereto. They are also entitled to correct any information held by us.

4. Operational Considerations

Monitoring

The Governing Body and Information Officer are responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. All employees, departments and individuals directly associated with us are to be trained, according to their functions, in the regulatory requirements, policies and guidelines that govern the protection of personal information. We will conduct periodic reviews and audits, where appropriate, to ensure compliance with this policy and guidelines.

Operating controls

We shall establish appropriate standard operating procedures that are consistent with this policy and regulatory requirements.

This will include:

- Allocation of information security responsibilities.
- Incident reporting and management.
- User ID addition or removal.
- Information security training and education.
- Data backup.

Policy Compliance

Any breach/es of this policy may result in disciplinary action and possible termination of employment.