CEDAR CREST NURSERY SCHOOL CC

MANUAL: POPIA POLICIES AND PROCEDURES

PREPARED IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT (NO 4 OF 2013)

COMPILED: 29/06/2021
REVISED: 29/06/2021

INDEX:

1. Introduction:

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy. The right to privacy includes a right to protection against unlawful collection, retention, dissemination and use of personal information.

In order to regulate the processing of personal information by public and private bodies in a manner that gives effect to the right of privacy subject to justifiable limitations that are aimed at protecting other rights and important interests, including the free flow of information within the Republic and across international borders, the Protection of Personal Information act No. 4 of 2013, ("the Act") was put into place.

The Act regulates the way personal information may be processed, by establishing conditions, in line with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information. It also provides persons with the rights and remedies to protect their personal information from processing that is not in line with the Act.

Within these pages we will set out our policies and procedures in terms of data collection, usage and restrictions, storage, security safeguards, responsibilities, complains and, retention and destruction.

Cedar Crest Nursery School CC ("the Responsible Party"), was registered on 21/12/2004 and conducts business as an early childhood development centre in the education sector.

Our role players are:

1. Data Subjects
    a. All clients (parents and children)
    b. All suppliers
    c. All employees

2. Responsible Party: Cedar Crest Nursery School CC

3. Operators
    a. Persons employed by the Responsible Party
    b. Third parties and software that perform certain functions for the Responsible Party, such as:
        i. Bookkeepers and Accountants/Auditors
        ii. Payroll packages
        iii. Accounting packages
    c. Third parties that require certain statutory submissions, such as:
        i. SARS
        ii. Labour Department
        iii. Department of Social Development

4. Information Officer: Arlene Adriaanse

5. Information Regulator: Government appointed

2. Application Provisions:

Please refer to the Protection of Personal Information Act.

3. Conditions for Lawful Processing:

Please refer to the Protection of Personal Information Act.

4. Data Collection:

In order to properly comply with statutory requirements and maintain a high level of service delivery, we need to process certain types of information of our employees, customers/clients and service providers.

Types of data:

Employees:
- CV
- Employment contract
- ID
- Contact details
- Banking details
- Income tax number
- Biographical information
- Salary information, leave records and Attendance registers

Customers/clients:
- Registered name, Trading name, Full names and surname
- Contact details
- Physical and/postal address
- Service agreement
- Service history
- Enrolment forms
- Consent forms
- ID and birth certificate copies

Service Providers:

- Registered name, Trading name, Full names and surname
- Contact details
- Physical and/postal address
- Banking details
- Non-disclosure agreement
- Service agreement/appointment letter

Purpose for data collection:

Processing of personal information is required to carry out actions for the conclusion or performance of a contract to which the data subject is party. Reasons for data collections includes, but is not limited to, the following:

- Compliance with obligations imposed on the Responsible Party by certain laws and regulations
- Protection of a legitimate interest of the Data Subject
- To pursue the legitimate interests of the Responsible Party or a third party to whom the data is supplied

Consent:

Personal information will only be processed if the data subject (or competent person where the data subject is a child) consents to the processing. The Responsible Party bears the burden of proof for such consent. The Data Subject may at any time withdraw their consent for processing only if the lawfulness of the processing of the information before such withdrawal is not affected. A Data Subject may object to processing personal information whereafter the Responsible Party may no longer process personal information.

Legal Aspects, Minimality & Transparency:

As a legal operating entity, the organisation is required by law to process certain data for each of the above data subjects. In order to comply with POPIA, the organisation will only process the exact information required in order to fulfil their duties to the data subjects and to comply with their legal and statutory obligations as a registered trading entity. All data subjects shall always be informed of the types of data held and the purpose for which it is held.

Personal information is to be processed lawfully and in a reasonable manner that does not infringe on the data subject. Personal information will only be processed if it is adequate, relevant and not excessive to the purpose for which it is processed.

5. Data Access and Accuracy:

The Responsible Party shall take reasonable practical steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

A Data Subject may at any time enquire from the Service Provider which data they hold for them. It is the duty of the Data Subject to inform the Service Provider of any data that has changed and needs to be updated.

The Data Subject shall inform the Service Provider of such changes in writing and provide the relevant supporting document(s) to confirm such change.

The Responsible Party shall not be held liable and/responsible for any inaccurate and outdated data used or losses incurred for the same reason.

6. Data Usage and Restrictions:

The Responsible Party and their authorised Operators shall process the data provided by the Data Subject for the sole purpose for which it was obtained initially. Such data shall also only be processed for the period that it is relevant.

The usage of data shall always be restricted to the purpose it was intended for. Should the Service Provider require personal information for another purpose, prior consent needs to be obtained from the Data Subject.

Only authorised Operators shall under the instruction of the Responsible Party be able to use personal information.

7. Data Storage:

Physical data records are stored in a locked filing cabinet on the premises. This includes all of the aforementioned records.

The responsible person does not store physical data records or electronic data records at an offsite location as such data records are securely stored on site. Access to such offsite data records are restricted to selected Operators mandated by the Responsible Party.

Electronic data records are stored on the computer at the premises. This includes contact details only.

The Responsible Party does not make use of cloud-based storage space.

8. Data Security Safeguards and Disclosure:

The Responsible Party has taken reasonable measures to ensure that all physical and electronic data records are safe and secure from unauthorised access and natural disasters.

Some of these measures include: Restricted access to data and confidentiality agreements.

Physical Data: All physical documents are locked away and only 2 people have keys and access to such.

Electronic Data (emails, computers/laptops, external drives, online storage): Data received via email shall be printed out and then deleted from email. Email address and contact details are maintained electronically and stored securely on password protected machines.

Servers (local and/or online): None

Passwords (restrict access to Operators): Yes

Should any of the Data held by the Responsible Party be compromised in any way (security breach or natural disaster), the Responsible Party shall inform the Information Regulator of such compromise as well as the affected Data Subjects in the prescribed manner.

Should there be a request for any data (physical or electronic) by any third party, the disclosure of such data shall be done in a lawful manner upon receipt of consent from the Data Subject to adhere to such request.

The requestor may also refer to the Responsible Party's PAIA manual for the procedures on requesting Data.

All requests shall be addressed to the Information Officer of the Responsible Party.

9. Responsibilities:

All operators of personal information shall always process such information only with the knowledge or authorisation of the Responsible Party and shall treat such information that comes to their knowledge as private and confidential. They may not disclose such information unless required by law or while performing their normal duties.

The Responsible Person shall, in the form of a written contract between the Responsible person and the Operator, ensure that the Operator establishes and maintains the security measures listed in point 8 above.

The operator must notify the Responsible Party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person.

The Responsible Party must ensure that all operators have been properly trained on the procedures and policies in terms of POPIA and PAIA in order to protect all personal information entrusted to them by the Data Subjects.

The Information Officer's responsibilities include the encouragement for compliance of the Responsible Party with the conditions for lawful processing of personal information and dealing with requests made to the Responsible Party in terms of the Act. The Information Officer will also work with the Regulator in relation to investigations conducted pursuant to prior authorisation.

10. Complaints:

Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject.

A responsible party or data subject may submit a complaint to the Regulator in the prescribed manner and form if they are aggrieved by the determination of an adjudicator, in terms of section 63(3).

A complaint to the Regulator must be made in writing.

Upon receipt of a complaint, the Regulator may conduct a pre-investigation and must inform the complainant and Responsible Party of the course of action to be taken.

11. Data Retentention and Destruction:

All data received from a Data Subject shall be retained for the duration of the service agreement between the Data Subject and Responsible Party.

Upon termination of such service agreement, the Responsible Party shall retain such personal information as required by relevant applicable legislation for a period of 7 years whereafter physical data records it will either be returned to the Data Subject or destroyed by the Responsible Party. Copies of electronic data records can be provided to the Data Subject upon their request, otherwise such records shall be permanently deleted by the Responsible Party.

Any data, physical or electronic, received that is not of use for the purpose of agreed upon service delivery processes will be returned and/or destroyed immediately.

12. Staff Awareness:

All currently employed employees shall be trained on all policies and procedures contained in this manual.

All new employees shall be trained on such policies and procedure as a part of their welcoming into the company.

Refresher sessions on such policies and procedures shall take place annually at the beginning of each new school year or as and when the Responsible Party deems necessary.