Confidentiality, Records & Popia (data Protection) Policy

Effective Date: 01/01/2025
Applies To: All prospective and enrolled families at **Besige Bytjie Akademie**

---

1. Purpose

This policy ensures that all personal, medical, educational, and financial information at Besige Bytjie Akademie is collected, stored, accessed, used, retained, and disposed of in a lawful, secure, and confidential manner. It aligns with the Protection of Personal Information Act (POPIA), 2013, and best practice in early childhood education to protect the privacy, dignity, and rights of children, parents/guardians, staff, and visitors.

---

2. Scope

This policy applies to:

- All staff, volunteers, management, and contractors at Besige Bytjie Akademie.
- All records relating to children, parents/guardians, staff, and visitors.
- All forms of records, whether physical or digital, including documents, databases, photographs, and correspondence.

---

3. Collection of Information

- Personal information is collected lawfully and only for specific, legitimate purposes related to education, care, safety, administration, and legal compliance.
- Only information necessary for preschool operations is collected, including:
    - Child details (name, date of birth, contact details)
    - Medical information (allergies, medication, pre-existing conditions)
    - Emergency contact details
    - Educational and developmental records
    - Financial information (fees, invoices, payment records)
- Parents/guardians are informed at enrolment about the types of information collected and the purpose for which it is used.

---

4. Types of Records

- **Child Records:** Personal details, medical information, developmental and educational reports, incident/accident reports.
- **Staff Records:** Personal information, employment contracts, performance evaluations, training records, and incident reports.
- **Financial Records:** Fee statements, receipts, and payment histories.
- **Health & Safety Records:** Accident and incident books, risk assessments, fire drill logs.
- **Communication Records:** Parent correspondence, consent forms, notices, and official communications.

---

5. Access to Records

- Access to records is strictly limited to authorised personnel on a need-to-know basis.
- Authorised access includes:
    - **Principal / Director:** Full access to all records.
    - **Class Teachers / Assistants:** Access only to records relevant to children in their care.
    - **Administrative Staff:** Access to records required for billing, attendance, and communication.
    - **Parents / Guardians:** Access to their own child's personal and educational records only, upon written request.
- Third parties (e.g., occupational therapists, social workers, or government authorities) may access records only with written parental consent or where required by law.
- Unauthorised access, sharing, copying, or discussion of records is strictly prohibited.

---

6. Storage and Security of Records

- **Physical Records:** Stored in locked filing cabinets in secure areas accessible only to authorised personnel.
- **Digital Records:** Stored on password-protected devices and secure cloud systems, encrypted where possible.
- Individual login credentials are issued to authorised staff; sharing of passwords is prohibited.
- Secure backups of essential digital records are maintained.
- Records are organised clearly to allow efficient and controlled retrieval.

---

7. Use and Sharing of Information

- Personal information is used only for the purpose for which it was collected (e.g., education, care, communication, safety, reporting, and administration).

- Information is not shared with third parties without parental consent unless required by law (e.g., emergency services, Department of Social Development, or other legal authorities).
- Staff receive guidance and training on confidentiality and POPIA responsibilities.

---

8. Confidentiality Guidelines

- Staff must not discuss any child's, parent's, or colleague's information outside of the preschool environment.
- Confidential information may not be shared on social media or with unauthorised individuals.
- All discussions regarding children or families must be professional and limited to authorised contexts.
- Breaches of confidentiality are regarded as serious misconduct and may result in disciplinary action.

---

9. Parental Rights

- Parents/guardians have the right to:
  - Access records held about their child, subject to identity verification.
  - Request correction or updating of inaccurate, incomplete, or outdated information.
- Requests must be submitted in writing to the Principal or designated Data Protection Officer.
- Parents are informed at enrolment about how records are stored, accessed, retained, and destroyed.

---

10. Retention of Records

- **Children's Records:** Retained until the child reaches at least 7 years of age.
- **Staff Records:** Retained for the duration of employment and for a minimum of 5 years thereafter, in line with labour legislation.
- **Financial Records:** Retained for a minimum of 5 years in compliance with SARS and accounting regulations.
- **Health & Safety Records:** Retained for at least 5 years or longer if required for legal or insurance purposes.

---

11. Destruction and Disposal of Records

- Records that are no longer required are securely destroyed to prevent unauthorised access.
  - **Physical Records:** Shredded or incinerated.
  - **Digital Records:** Permanently deleted from systems and backups.
- Disposal is documented, including the date, type of record, and responsible staff member.

---

12. Data Breach Procedure

- Any suspected or confirmed data breach must be reported immediately to the Principal or Data Protection Officer.
- The breach will be investigated promptly.
- Affected parties and authorities will be notified as required by POPIA.
- Corrective measures will be implemented to prevent recurrence.

---

13. Staff Responsibilities

All staff and authorised persons must:

- Adhere to this policy at all times.
- Handle personal, medical, educational, and financial information confidentially.
- Report any suspected breaches, risks, or concerns immediately.
- Participate in regular POPIA and data protection training.
