

SPRINGVALE PRIMARY SCHOOL

Established 1981



PERSEVERE

POLICY PROTECTION OF PERSONAL INFORMATION

13. APPROVAL

Designation	Reviewer: Name & Surname	Signature	Date noted
School Principal	J. RAJKUMAR		5/08/2024
SGB Chairperson	DANNY MATHESWARA		5/08/2024
ISSP: Policy & Planning			
Circuit Manager			
Cluster Manager			
District Director			

Table of Contents

1. TITLE OF THE POLICY	3
2. EFFECTIVE DATE:.....	3
3. DATE OF NEXT REVIEW:	3
4. REVISION HISTORY:	3
5. PREAMBLE.....	3
6. PURPOSE AND OBJECTIVE OF THIS POLICY	4
7. DEFINITIONS AND ACRONYMS.....	4
8. APPLICATION AND SCOPE OF THE POLICY	8
9. LEGISLATIVE FRAMEWORKS AND POLICIES:.....	8
10. RELEVANT POLICIES AND PROVINCIAL CIRCULARS.....	9
11. POLICY STATEMENTS	10
12. SHORT TITLE.....	16
13. DATE OF APPROVAL.....	17
ANNEXURE A	18
ANNEXURE B	20
ANNEXURE C	21

1. TITLE OF THE POLICY

PROTECTION OF PERSONAL INFORMATION AND THE RETENTION OF DOCUMENTS AND RECORDS.

2. EFFECTIVE DATE:

AUGUST 2024

3. DATE OF NEXT REVIEW:

The Governing Body will review this policy every three years or sooner if there is a change in the relevant legislative framework; or for operational reasons whenever circumstances so require; or at the request of the Head of Department

4. REVISION HISTORY:

July 2024 – SGB approval 29 July 2024

5. PREAMBLE

- **Objective:** The Protection of Personal Information Act (POPIA) aims to ensure personal information is processed fairly and does not infringe on the rights of individuals.
- **Applicability:** All personal data processing must comply with POPIA.
- **School Details:** Springvale Primary is a public school governed by the South African Schools Act, offering education in grades R to 7 with languages as the medium of instruction.
- **Privacy Rights:** The school values privacy and is committed to managing personal information in line with POPIA.
- **Balance:** POPIA balances the school's need to process personal data with individuals' privacy rights.
- **Importance:** Lawful processing of personal information is crucial for effective service delivery and maintaining trust.
- **Compliance:** The school adheres to POPIA principles and relevant regulations, emphasizing ethical and effective use of personal data by all staff.

Contact Information:

- **Address:**
- **Street:** 294 Friederich Street, Wierda Park, Centurion, 0149
- **Postal:** P.O. Box 517, Wierda Park, Centurion, 0149
- **Phone:** 012 6600024
- **Email:** springvale.admin@springvale.co.za
- **Information Officer:** C.D J. Rajkumar, ashar@springvale.co.za
- **Deputy Information Officer:** S. Khan, springvale.admin@springvale.co.za

6 PURPOSE AND OBJECTIVE OF THIS POLICY

- **Safeguarding Personal Information (Policy 6.1):** Purpose: To protect the personal information held by the school from threats, whether internal or external (deliberate or accidental), thereby safeguarding the privacy rights of all Data
- **Protection of School Records (Policy 6.2):** Purpose: Ensure the continuity of day-to-day school operations by safeguarding the school's records and information
- **Regulation of Personal Information Processing (Policy 6.3):** Purpose: Establish guidelines for how personal information is processed within the school. It specifies the purposes for which collected information can be used.
- **Appointment of Information Officers (Policy 6.4):** Purpose: Appoint Information Officers responsible for promoting, enforcing, and fulfilling the rights of Data.
- **Compliance Risks Mitigation (Policy 6.5):** Purpose: Protect the school from compliance risks related to personal information protection. These risks include:
 - - **a. Breaches of Confidentiality:** If personal information is inappropriately shared or disclosed, it could lead to revenue loss for the school.
 - **b. Lack of Choice:** Data Subjects should have the freedom to decide how their information is used.
 - **c. Reputational Damage:** Unauthorized access to personal information could harm the school's reputation

7. DEFINITIONS AND ACRONYMS

7.1. DEFINITIONS:

TERM	EXPLANATION
Accessibility of Data	Ease of obtaining data.
Accuracy of Data	Degree to which data correctly represents the intended information.
Administrative Data	Data from administrative sources.
Advanced Electronic Signature	An electronic signature accredited by an Authority under ECTA.
Anonymisation	Altering personal data so that individuals cannot be identified.
Archive	Repository for physical or digital documents and data.
Authentic Records/Documents	Records proven to be genuine and considered official.
Authoritative Records/Information	Records that are complete, dependable, and unaltered.
Automated	Equipment that processes information automatically.
Automated Transaction	Electronic transaction performed without human review.
Best Interests of the Child	Primary consideration in processing a child's information.
Biometrics	Identification technique based on physical or behavioural traits.
Bots/Chatbots	Automated programs mimicking human interactions online.
Browser	Program that accesses and reads data on the Internet.
Child	A natural person under 18 who cannot make decisions independently.

Certified Copy	Copy of a document verified as a true copy, not necessarily as genuine.
Circuit Manager	Head of an education circuit within the district.
Competent Person	Legally able person to consent on behalf of a child.
Confidential Information	Information that should be kept confidential, not limited to personal information.
Consent	Freely given, informed agreement for processing personal data.
Constitution	The Constitution of South Africa, 1996, as amended.
Custody of Records/Documents	Control of records/documents based on physical possession.
Data	Electronic representations of information.
Data Breach	Unauthorized or accidental destruction, loss, or disclosure of personal data.
Data Confidentiality	Extent to which unauthorized disclosure of data is harmful.
Data Credibility	Quality or power of data to be believed as true.
Data Message	Information generated, sent, received, or stored electronically.
Data Subject	Individual or entity to whom personal information relates.
De-Identify	Removing identifiers from personal data to prevent identification.
Deputy Principal	Educator assisting and substituting for the principal.
Disposal	Action of destroying or transferring records/documents.
Direct Marketing	Approaching individuals to promote goods/services or request donations.
Education District Office	District Office of the GDE where the school is located.
District Director/Manager	Officer responsible for education administration in a district.
Document	Any recorded information regardless of form or medium.
Domain Name	Alphanumeric designation for an Internet address.
Domain Name System	System that translates domain names into IP addresses.
Education	Learning undertaken in a registered educational institution.
Education Management	Organizing teaching and learning activities in a school.
Education Management Information System (EMIS)	System for organizing educational management information.
Educator	Person teaching or providing educational services.
Electronic Communication	Messages sent electronically via various devices and platforms.
Electronic Records/Data/Information System	Components of an electronic information system.
Electronic Transactions/Payments	Includes electronic communication and financial transactions.
E-mail	Electronic mail messages exchanged online.
Enrolled Learner	Learner admitted and recorded in the school's register.
Expression of Will	Data subject's clear agreement to provide information.
File Plan	Classification plan for organizing records/documents.
Filing System	Structured set of personal information for storage and retrieval.
School Governing Body	Governing body of the school as defined by SASA.
Historical Data	Data that is two or more years old.
Home Page/Web Site	Primary entry point of a web page or site.

Hyperlink	Reference linking to another data message or web page.
Information	Data presented in context for use.
Information Matching Programme	Comparing documents containing personal information to verify or produce new information.
Information Officer	Person responsible for ensuring compliance with POPIA in the school.
Information Regulator	Regulator established under POPIA.
Informed	Data subject is properly informed about the information being processed.
In Loco Parentis	Acting in place of a parent during school activities.
Judgment	Court decision resolving disputes and explaining orders.
Juristic Person	Entities like partnerships or companies represented by the SGB.
Learner	Person receiving or required to receive education at the school.
Learner Profile	Record of a learner's progress and development.
Member of the Executive Council	MEC for Education in Gauteng Province.
Member of Staff/Staff Member	Person employed at the school.
Mobile social media	Social media accessed via mobile devices.
Operator	Person processing data on behalf of the school under contract.
Parent/Guardian/Caregiver	Biological, adoptive, or legal guardian of a learner.
Person	Natural person or juristic person.
Personal Information	Information relating to an identifiable natural or juristic person.
Personal Identifiable Information/Online Identifier	Any identifier that can identify a data subject.
Policy Manual	Privacy and Protection of Personal Information Policy Manual.
Prescribed	As specified by regulation or code of conduct under POPIA.
Principal	Head of the school.
Private Body	Non-public body such as a person or partnership engaged in trade or business.
Privilege	Right to withhold or refuse to divulge confidential information.
Processing	Operations related to handling personal information.
Professional Legal Adviser	Legal professional providing independent, confidential advice.
Protection of Personal Information Act (POPIA)	South African law governing the processing of personal information.
Public Body	Governmental or public institution or functionary.
Public Record	Record created or received by a public body during its activities.
Pseudonymisation	Processing data so it can't be linked to a specific individual without additional information.
Public Record	Record in the public domain under control of a public body.
Recipient	Person or entity receiving personal data.
Record	Any recorded information regardless of form or medium.
Recording	Media on which sounds or images are captured.
Regulator	Information Regulator established under POPIA.
Re-identify	Restoring the ability to identify a previously de-identified data subject.
Representative	Person designated to provide information or sign documents on behalf of another.

Responsible Party	Entity determining the purpose and means for processing personal information.
Restriction	Withholding personal information from use or publication without deletion.
Retention Period	Time records are kept before archival or destruction.
Scanned Document/Document Scanning	Converting paper documents into digital format.
School	Irene Primary School, enrolling learners from grades R to 7.
School Activity	Official educational or recreational activity of the school.
School Fees	Monetary contributions related to school attendance or participation.
Sensitive Data	See Special Personal Information.
Sibling	Person with a shared parent and living in the same household.
Signature	Includes electronic and stylized representations of a person's name for signing documents.
Social Media Platforms/Sites/Apps	Websites and apps for creating online communities and sharing content.
Social Media Services	Web-based services accessed via various devices for interaction and content sharing.
Special Personal Information	Sensitive personal information including beliefs, race, health, and criminal behaviour.
Specific	Precise and detailed information requested and processed for a clear purpose.
Submit	Methods of sending information/documents: data messages, electronic communication (with receiver notification), telephone records, registered post, electronic mail, facsimile, personal delivery.
Surveillance Cameras (CCTV)	Cameras used by the school to monitor movements and behaviour through video and audio footage. Details are in the CCTV Policy and signposted at entrances.
Third-Party	Any person or entity, other than the data subject or authorized school personnel, involved in processing personal data.
Unique Identifier	A specific identifier assigned to a data subject that uniquely identifies them in relation to the responsible party.
User-generated Content	Electronic content created by users, including text posts, comments, photos, videos, and data from online interactions.
Voluntarily	Consent must be given freely by a data subject, without pressure, unless legally permitted otherwise.
Web Page	A data message available on the World Wide Web.
Web Site	A location on the Internet with one or more web pages.
World Wide Web (www)	An information browsing system allowing access to and linking between information on remote computers or devices.
Writing	Includes data messages that are accessible and usable for future reference, as per the Electronic Communications and Transactions Act.

7.2. ACRONYMS:

Acronym	Explanation
App	Application Software used for access to a social media platform/software programme.
ATM	Automatic Teller Machine
CCTV	Closed Circuit Television (Cameras, viewing screens and recording equipment) aka Surveillance Cameras
DBE	Department of Basic Education
DPIA	Data Protection Impact Assessment
ECTA	Electronic Communications and Transactions Act, Act 25 of 2002
EFT	Electronic Financial Transaction
EMIS	Education Management Information System
FAQs	Frequently Asked Questions
FEDSAS	Federation of South African Schools
GBF	Governing Body Federation
GDE	Gauteng Department of Education
MEC	Member of the Executive Council for Education in the Gauteng Province.
NAPTOSA	National Professional Teachers' Organisation of South Africa
POPIA	Protection of Personal Information Act, 2013
PII	Personally, Identifiable Information
PSA	Public Service Association
SADTU	South African Democratic Teachers' Union
SAOU	Suid-Afrikaanse Onderwysersunie
SASA	South African Schools Act, 1996
SBST	School-Based Support Team
SGB	School Governing Body
SMT	School Management Team
UGC	User-generated Content on any social media platform and/or using and posting data/information on any social media platform.

8. APPLICATION AND SCOPE OF THE POLICY

9. LEGISLATIVE FRAMEWORKS AND POLICIES:

- 9.1. Constitution of the Republic of South Africa, Act 108 of 1996.
- 9.2. South African Schools Act, Act 84 of 1996.
- 9.3. National Regulations for Safety Measures at Schools, GN 1040 of 2001, as amended.
- 9.4. The Protection of Personal Information Act no 4 of 2013, as amended.
- 9.5. South African Council of Educators Act, 2000(Act No. 31 of 2000), as amended.
- 9.6. Public Service Act, 1994, as amended.
- 9.7. General Notice 6903 of 2000 as amended, Misconduct of Learners at Public Schools and Disciplinary Proceedings.
- 9.8. General Notice 1040 of 12 October 200, as amended, Regulations for Safety Measures at Public Schools.
- 9.9. National Health Act, 2003 (Act No 61 of 2003), as amended and related regulations.
- 9.10. School Education Act, 1995 (Act 6 of 1995), as amended.

- 9.11. General Notice 1189 of 2012, Regulations on Domestic and International Tours for Learners at Public Schools, 2012.
- 9.12. Electronic Communications and Transactions Act, 25 of 2002.
- 9.13. Financial Intelligence Centre Act, Act 38 of 2001, as amended.
- 9.14. Compensation for Occupational Injuries and Diseases Act, Act 130 of 1993, as amended.
- 9.15. Basic Conditions of Employment Act, Act 75 of 1997.
- 9.16. Employment Equity Act, Act 55 of 1998.
- 9.17. Labour Relations Act, Act 66 of 1995 and Codes of Good Practice.
- 9.18. Unemployment Insurance Act, Act 63 of 2002.
- 9.19. Tax Administration Act, Act 28 of 2011.
- 9.20. Income Tax Act, Act 58 of 1962.
- 9.21. Skills Development Levies Act, Act 9 of 1999.
- 9.22. Securities Services Act, Act 36 of 2004.
- 9.23. The Control of Access to Public Premises and Vehicles Act 1985 (Act No. 53 of 1985), including regulations made under it ("the Public Premises Act").
- 9.24. General and Further Education and Training Quality Assurance Act.
- 9.25. Regulations pertaining to POPIA.
- 9.26. Umalusi Policy and Criteria.
- 9.27. National Archives and Records Service of South Africa Act, (Act No 43 of 1996), as amended.
- 9.28. Guidance Notes on the Processing of Personal Information in the Management and Containment of Covid-19 Pandemic in Terms of the Protection of Personal Information Act 4 of 2013 issued by the Information Regulator of South Africa.
- 9.29. National Education Policy Act, 1996, Act 27 of 1996, as amended.
- 9.30. The Criminal Procedure Act, Act 51 of 1977.
- 9.31. The Films and Publications Act, Act 65 of 1996, as amended.
- 9.32. Employment of Educators Act, 1998, Act 76 of 1998, as amended.
- 9.33. Regulation of Interception of Communications and Provision of Communication-Related Information Act, Act 70 of 2002.
- 9.34. Government Notice 487 dated 6 June 2011 - SC006: Dictionary of Education Concepts and Terms published by the Minister of Basic Education.
- 9.35. Copyright Act, Act 98 of 1978.
- 9.36. Short Term Insurance Act, Act 53 of 1998.

10. RELEVANT POLICIES AND PROVINCIAL CIRCULARS

- 10.1. School Health and Safety Policy.
- 10.2. Admission Policy of the School.
- 10.3. Language Policy of the School.
- 10.4. Religion Policy of the School.
- 10.5. Code of Conduct for Learners and related rules and policies of the school.
- 10.6. Extramural and Sports Policy of the School.
- 10.7. Transport Policy of the School.
- 10.8. Asset Register of the School.
- 10.9. COVID-19 Protocol and Anti-Stigmatisation Policy of the School.
- 10.10. HIV/AIDS, TB and STI's Policy of the School.
- 10.11. Domestic and International Tours Policy of the School.
- 10.12. Privacy Policy of the School.
- 10.13. School Social Media Policy.
- 10.14. School CCTV Policy.
- 10.15. Code of Conduct for Parents and Visitors of the School.
- 10.16. Personnel Administrative Measures.
- 10.17. SACE Code of Conduct and the Code of Conduct for Public Servants.

Springvale Primary School – Protection of Personal Information Policy

The information contained within this document is confidential and for the exclusive use of Springvale Primary School

10.18. Contractual obligations of employees employed by the SGB.

10.19. GDE Memorandum – Requirements for Storage of Examination Materials at the District Offices and Examination Centres - 2014

11. POLICY STATEMENTS

11.1. Key Principles of the Policy Manual

- **Change in Culture:** POPI requires a shift in school culture and a consistent effort rather than a one-time event.

- **Compliance Requirements:**
 - **Management Will:** Commitment from school management.
 - **Staff Training:** Regular training and re-training.
 - **Process Management:** Regular inspection and management of information processes.
 - **Reporting:** Measure and report on information management.
 -

11.2. Commitment to POPIA Principles

- **Transparency:** Clearly define procedures for handling personal information.
- **Regulatory Compliance:** Adhere to all relevant laws and regulations

- **Lawful Collection:** Collect personal information fairly and lawfully, ensuring it aligns with its intended purpose.
- **Notification:** Inform individuals when their personal information is collected.

- **Special Care:** Handle sensitive personal information with extra care.
- **Consent:** Obtain consent when required to process personal information.

- **Accuracy:** Ensure personal information is accurate and up to date.
- **Security:** Implement safeguards against risks like unauthorized access or destruction.

- **Access and Correction:** Allow individuals to access and correct their personal information.
- **Third-Party Sharing:** Share information only with parties who have adequate privacy and security measures.

- **Transfer Compliance:** Follow rules for transferring information both nationally and internationally.
- **Employee Awareness:** New employees must be informed about their responsibilities under POPIA during induction or training.

11.3. The School as a Public Body

- **Status:** The school is part of the State, with some independent powers.
- **Administration:** It is part of the GDE (Gauteng Department of Education)
- **Legal Function:** Acts under the Constitution of South Africa and provincial legislation.

11.4. Principles of Compliance

- **Consent:** Obtain consent before collecting or processing data.
- **Purpose Limitation:** Collect only the data needed for legitimate purposes.
- **Purpose Matching:** Use data in ways consistent with its collection purpose.
- **Security:** Implement reasonable security measures to protect data.
- **Storage:** Retain information only as long as necessary.
- **Rights:** Ensure data subjects can access and correct their information.

11.5. Privacy Policy and Privacy Notice

- **Privacy Policy:** Details handling practices and staff obligations for processing personal information.
- **Privacy Notice:** Communicates the school's data privacy mission and practices to external stakeholders and data subjects.

11.6. Specific Purpose Collection of Information

Purpose Limitation: Personal information must be collected for a specific, lawful purpose related to the school's functions. Data subjects must be informed of this purpose.

11.7. Rights of Data Subjects

Awareness: The school will ensure data subjects are aware of their rights under POPIA, including:

- **Notification:** Right to be informed when personal information is collected or accessed by unauthorized parties.
- **Access:** Right to know if the school holds their personal information and to request access to it.
- **Correction/Deletion:** Right to request correction, destruction, or deletion of their personal information.
- **Objection:** Right to object to processing based on personal grounds or for direct marketing.
- **Automated Decisions:** Right not to be subjected to decisions based solely on automated processing.
- **Complaint:** Right to submit complaints to the Regulator or initiate civil proceedings regarding interference with personal information protection.

11.8. Caution for Parents/Guardians/Caregivers

Privacy Responsibility: Laws protecting learner information do not extend to personal disclosures made by parents or learners. They should use privacy tools and maintain secure online practices to protect their information from unauthorized access.

11.9. Processing of Information

Scope: POPIA applies to all personal information processed by the school, whether by automated or non-automated means, if it is part of a filing system.

11.10. Information Security Measures

- **Technology and Security:** The school employs up-to-date security measures to protect personal information, including:
 - **Firewalls**
 - **Virus Protection Software**
 - **Access Control**
 - **Secure IT Infrastructure**
 - **Regular Security Controls by Third Parties**

11.11. POPIA's Eight Conditions for Lawful Processing

1. Accountability

- The school is responsible for ensuring compliance with all POPIA conditions and must manage data processing responsibly.

2. Processing Limitation

- Data must be processed with respect for privacy, relevance, and consent. Data should be collected directly from the data subject unless specific exceptions apply.

3. Purpose Specification

- Data collection must be for a clear, lawful purpose related to the school's activities. The school must inform data subjects of the purpose and not retain data longer than necessary.

4. Further Processing Limitation

- Further processing of data must align with its original purpose. Additional processing is allowed if consented to, required by law, or related to public interest.

5. Information Quality

- Data must be accurate and complete.

6. Openness

- The school must inform data subjects about the data collection process, including the purpose, source, and whether data provision is voluntary.

7. Security Safeguards

- Implement appropriate measures to protect data from unauthorized access, loss, or damage. This includes physical and electronic security, maintaining records, and notifying breaches.

8. Data Subject Participation

- Data subjects have the right to access, correct, or request deletion of their personal information. Processing of special data categories has additional conditions and exemptions.
-

11.12. Data of Children

Personal information of children can only be processed with consent from a competent person, for legal obligations, or under specific circumstances like public interest or research.

11.13. Access and Security to Information/Records

• General Security:

- Records must be protected from unauthorized access. Only authorized personnel can manage classified records, and removal or disclosure of records must be approved.

- **Paper-Based Records:**

- Must be securely managed and not altered without permission. Tampering with records results in disciplinary action.

- **Electronic Records:**

- Must be kept secure with proper access controls and regular updates. Loss or theft of devices must be reported immediately.

11.14. Performing a POPIA GAP Analysis and Risk Assessments

- **Purpose:** Identify compliance gaps and assess risks related to data protection.
- **Scope:** Evaluate the school's IT infrastructure and data handling practices to ensure they meet POPIA requirements. Address data collection, use, sharing, and storage practices.
- **Assessment Questions:** Verify legal authority, consent, relevance of data, third-party disclosures, and data disposal processes.

11.15. Drafting and Updating Policies

- **Required Documents:** Include Privacy Policy, Information Security Procedures, Incident Response Policy, Information Manual, and Reporting Procedures.
- **Communication:** Share updated policies with staff and third-party partners to ensure compliance with POPIA.

11.16 Compliance Management

- **Ongoing Process:** Compliance is a continuous process requiring active management.
- **Regular Updates:** Schools must have a systematic plan to review and update processing standards regularly.
-

11.17 Consent to Process Personal Information

- **Legal Duty:** Schools must process personal information lawfully under POPIA.
- **Required Consent:** Express and informed consent is needed to process personal information, except in specific situations such as contractual obligations or legal requirements.
- **Legal Exceptions:** Processing without consent is permitted in cases like compliance with various laws, protecting legitimate interests, and specific regulatory requirements.

11.18 Signature and Document Procedures

- **Signatures:** The signer must understand and agree to the document's contents, ensure completeness, and be aware of the binding nature of their signature.
- **Invalid Signatures:** Electronic signatures may not be acceptable for all documents.
- **Mark or Thumbprint:** For those unable to sign, a mark or thumbprint can be used, potentially in the presence of a commissioner of oaths or notary.

- **Representative Signing:** Authorized representatives can sign on behalf of others or entities.

11.19 Witnessing Document

- **Purpose:** Witnesses verify the identity and authenticity of signatories to prevent fraud.
- **Requirements:** Witnesses must ensure the signatory is present, use black ink, initial changes, and provide necessary details.
- **Evidentiary Use:** Witnesses can confirm signatures in legal disputes.

11.21 Common Acts of POPIA Non-Compliance

Examples: Includes loss or theft of data, insecure web pages, unauthorized email disclosures, and poor handling of physical and digital documents.

11.22 POPIA and Email Usage

- **Usage:** School email accounts are for school-related purposes. Personal use is limited and subject to the same policies.
- **Ownership and Integrity:** Emails are school property; users are responsible for mailbox integrity. Confidentiality cannot be guaranteed.
- **Security:** Caution with attachments, avoid defamatory content, and handle suspect emails carefully. Unauthorized reading or forwarding of emails is prohibited.

11.23 POPIA and Bulk Email

Guidelines: Bulk emails must be courteous, non-commercial unless authorized, and relevant to the school's purpose. Personal and inappropriate content should be avoided.

11.24 POPIA and Internet Usage

Permitted Use: Internet access is for school-related activities and professional development. Personal gain, illegal activities, and unauthorized advertising are prohibited.

11.25 POPIA and Personal Websites

- **Academic Freedom:** Staff can maintain personal sites but must not use school trademarks without permission or present personal views as official school positions.
- **Prohibitions:** Sites should not breach laws, damage the school's reputation, or infringe on third-party rights. Staff must clearly state that personal views are not the school's official stance

11.26 Retention of Personal Information Records:

The school will keep personal information records as mandated by relevant legislation, such as the Archives Act and POPIA, unless a data subject requests a shorter retention period.

11.27 Records Search and Notification:

If records cannot be found, the requester will receive an affidavit detailing the search efforts and confirming the record's non-existence.

11.28 Scanned Documents:

Hard copies of scanned documents must be retained for 1 year, with exceptions for staff-related documents, which must be kept for 3 years post-employment.

11.29 Monitoring and Implementation:

The SGB, SMT, Principal, and Information Officer are responsible for implementing and monitoring this policy, including periodic reviews for compliance.

11.30 Operating Controls:

The school will establish privacy controls covering responsibilities, incident management, user access, training, and data backup.

11.31 Reporting Vulnerable Children:

Professionals must report any child at risk to the principal, SAPS CPU, or Social Services, following the Children's Act.

11.32 Notifying Parents of Learner Harm:

The principal must inform relevant parties if a learner is harmed due to certain activities, respecting limits on personal information sharing.

11.33 Occupational Health and Safety:

Under the Occupational Health and Safety Act, the SGB or principal must inform employees of any health or safety dangers.

11.34 Certified Copies:

Certified copies must be stamped and signed by authorized officials, with specific requirements for certification, to prevent fraud and document loss.

11.35 School Photographs/Images/Videos:

Photographs and images of learners are personal information. Parental consent is required for third-party release, and images on the school's website must be protected from copying.

11.36 SGB Employees' Information:

SGB employees must sign agreements covering consent and confidentiality for handling their personal information. Non-compliance may lead to disciplinary action.

11.37 CCTV:

CCTV is used for security and crime prevention. Notices will be posted, and recordings will be retained per the school's retention policies.

11.38 Entry to School Grounds:

The school may inspect persons and property, record visitor details, and refuse entry at the principal's discretion.

11.39 Bots:

Bots may be used responsible for managing emails and FAQs on social media and the school's website.

11.40 Direct Marketing by Unsolicited Electronic Communications:

- Direct marketing using personal information is **prohibited** unless consent is obtained from the data subject or if they are already a parent of the school, a prospective parent, or someone requesting information.
- Consent must be sought only once and only used for the intended purpose.
- Marketing communications must include the sender's identity, contact details, and opt-out information. If not all information fits in a message, a link to a webpage with details can be used.
-

11.41 POPIA Complaints Procedure:

Complaints about POPIA violations can be submitted via email to the school at admin@ireneprimary.co.za.

11.42 Destruction of Documents:

- Documents should be shredded or otherwise destroyed after the retention period. Each department is responsible for regular destruction of documents and ensuring no important originals are lost.
- Destruction must be logged, and electronic records should be securely deleted with IT Department consultation.
-

11.43 Disciplinary Action:

- Post-investigation, appropriate administrative, legal, or disciplinary action will be taken for non-compliance with POPIA.
- Ignorance or minor negligence will result in additional training. Gross negligence or wilful misconduct may lead to serious disciplinary actions as per Employment Act procedures.

11.44 Personal Information No Longer Personal Information:

De-identified personal information and the personal information of deceased persons are not considered personal information under POPIA.

11.45 Encryption of Personal Information:

All electronic personal information must be encrypted and password-protected to ensure security and compliance with POPIA.

11.46 Information Held in the Cloud:

To reduce risks, personal information should be consolidated into a single encrypted cloud location with controlled access.


11.47 Data Portability:

Data subjects have the right to move or copy their personal data in a structured, commonly used format between data controllers or IT systems, as per Section 20 of POPIA.

12. SHORT TITLE

This Policy will be known as the POPIA Policy of the School.

13. DATE OF APPROVAL

Designation	Reviewer: Name & Surname	Signature	Date noted
School Principal	J. Rajkumar	J. RAJKUMAR	5/08/2024
SGB Chairperson	D. Mathebula		5/08/2024
ISSP: Policy & Planning			
Circuit Manager			
Cluster Manager			
District Director			

ANNEXURE A

Summary of Personal Information and Records Held by the School

1. Learners

- **Personal Details:** Names, ID numbers, birth dates, gender, race, contact info, medical info, disabilities, home language, and contact details.
- **Documents:** Birth certificates, ID documents, inoculation certificates, report cards, permits, etc.
- **Records:** Profiles, transfer cards, disciplinary records, merit records, academic records, behavioural records, photographs, biometrics, CCTV footage, and special education data.

2. Parents

- **Personal Details:** Names, ID numbers, birth dates, gender, race, marital status, medical aid, contact info, profession, employment, and children's names.
- **Financial Records:** School fee accounts, exemption applications, financial documents.
- **Documents:** Correspondence, CCTV footage.

3. Employees (School/SGB)

Personal Details: ID documents, qualifications, contact details, banking details, CVs, references, contracts, performance appraisals, medical records, payroll records, disciplinary records, biometrics, police clearance.

4. Employees (State) Personal Details: ID documents, PERSAL numbers, contact details, qualifications, salary scales, CVs, performance appraisals, medical records, payroll records, police clearance.

5. Learnerships/Students/Assistant Educators Personal Details: ID documents, contact details, contract agreements, performance appraisals, banking details, and police clearance.

6. Temporary Staff Personal Details: ID documents, CVs, contact details, contracts, banking details, payroll records, and police clearance.

7. Suppliers/Agents/Contractors Personal Details: Information of suppliers, financial records, contracts, correspondence, tender documents.

8. School Governing Body (SGB) Personal Details: Contact details, SGB constitution, budgetary info, minutes, agendas, and policies.

9. Tenants Personal Details: Lease agreements, correspondence, contact details, and payment account details.

10. Government Departments Documents: Legislation, circulars, guidelines, policies, meeting minutes, records of school evaluations, and financial reports.

11. Past Learners/Alumni Personal Details: Contact info, newsletters, transfer cards, and academic records.

12. Sponsors/Donors/Supporters Personal Details: Contact details, receipts, donation register, correspondence.

13. Advertisers Personal Details: Contact details, invoices, advertisement details, and correspondence.

14. Sporting/Cultural Bodies Personal Details: Contact details, subscriptions, correspondence, sporting codes, and financial transactions.

15. Academic Authorities/Associations Personal Details: Contact details, subscriptions, registration lists, correspondence.

16. SGB Associations Personal Details: Contact details, newsletters, subscriptions, correspondence.

17. Unions Personal Details: Contact details, subscriptions, case records, and correspondence.

18. Statutory Bodies Personal Details: Contact details, statutory returns, payment records, IRP5s.

19. School Auditors Personal Details: Contact details, audit reports, contract of service, financial statements, correspondence.

20. Insurance Houses Personal Details: Contact details, insurance agreements, claim forms, and correspondence.

21. Banking Institutions Personal Details: Contact details, records of accounts, transactions, cheque books, and banking fees records.

- 22. Attorneys/Debt Collectors Personal Details:** Contact details, case records, contracts, and correspondence.
- 23. Outsourced Payroll Personal Details:** Contact details, contract, financial records, and correspondence.
- 24. Outsourced Cleaning/Other Services Personal Details:** Contact details, contracts, payment statements, and correspondence.
- 25. Outsourced IT/Office Equipment Personal Details:** Contact details, contracts, service records, and correspondence.
- 26. Trustees/Old Boys/Girls/Supporters' Clubs Personal Details:** Trustee/member info, trust documents, records of donations, and correspondence.
- 27. Hostel Records Personal Details:** Staff and boarders' info, conduct codes, payment records, attendance registers, and correspondence.
- 28. Educational Institutions Documents:** Institution info, contact details, and correspondence.
- 29. Information Technology Documents:** IT policies, network diagrams, user manuals, software licenses, antivirus software.
- 30. School Records Documents:** School constitution, strategic plans, class lists, policies, financial records, incident records, curriculum documentation, asset registers, and software records.

