Sunward Christian Academy (SCA)
POPI School Policy and Procedures

Policy Date	June 2021

1. INTRODUCTION

This Data Protection and Information Sharing Policy describes the way that SCA will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013, as that is the key piece of legislation covering security and confidentiality of personal information. as well as PAIA -The Promotion of Access to Information Act 2 of 2000.

1.1. POPI and PAIA

The Promotion of Access to Information Act (PAIA) was passed to give effect to the constitutional right of access to information that is held by a private or public body and that is required for the exercise or protection of any rights.

The Protection of Personal Information Act (POPI) was enacted to give effect to the constitutional right to privacy by promoting the protection of personal information when processed by public or private bodies.

SCHOOL Details

Head of School:	Mr Leon van der Westhuizen
Information Officer Contact email Contact number	Mr Leon van der Westhuizen info@scacademy.co.za 011 896 1276
School Physical Address	Cnr Trichardt & Schreiner street, Parkrand Village Boksburg
School Telephone Number	011 896 1276
School POPI email address	info@scacademy.co.za

2. DEFINITIONS

1.1. Consent	means the voluntary, specific and informed expression of will
1.2. Data Subject	means the natural or juristic person to whom the Personal Information relates
1.3. Direct Marketing	means approaching a Data Subject personally for the purpose of selling them a product or service, of requesting a donation;
1.4. POPI	means the Protection of Personal Information Act, No. 4 of 2013
1.5. PAIA	means The Promotion of Access to Information Act 2 of 2000
1.6. Personal Information	means information relating to an unidentifiable, living, natural person, or an identifiable, existing juristic person, as defined in POPI;
1.7. Processing	means an operation or activity, whether or not by automatic means, concerning Personal Information.
1.8. Minimality	only the minimum amount of personal information that is necessary ('adequate, relevant and not excessive') for the purpose for which the information is needed, should be collected and processed.
1.9. De-identify	means to delete any information that – - Identifies the data subject; - can be used or manipulated by a reasonably predictable method to identify the data subject; or

	- can be linked by a reasonably conceivable method to other information that identifies the data subject, and whereas,
1.10. Re-identify	means to resurrect any information that has been de-identified.
1.11. Record	A record is a form of recording of information, regardless of the medium on which it is recorded, that is under the control of a responsible party.

3. SCOPE OF THE POLICY

The Policy applies to all SCA employees, Board Members, 3rd party suppliers and Parents. The provisions of the Policy are applicable to both on and off-site processing of personal information.

4. POLICY STATEMENT

SCA collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out the business of education effectively. SCA regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between SCA and those individuals and entities who deal it. The School will endeavour to comply with the law and follow good practise in respect of the data it holds about individuals. The school will endeavour to protect its employees and Data Subjects connected to the school whilst protecting the school from the consequences of a breach of its responsibilities.

5. PROCESSING OF PERSONAL INFORMATION

5.1. Purpose of Processing

SCA uses the Personal Information under its care in the following ways:

- Processing of applications of school children by parents/ guardians
- Record of Parent / guardian details of enrolled school children
- Record of parent / guardian financial account with school
- Record of enrolled child details
- Record of enrolled child educational details/ history
- Processing of applications for employment at the school
- Record of staff details
- Staff administration
- Submission of learner statistics to the Department of Education and Associations
- Complying with legal and regulatory requirements

5.2. Categories of Data Subjects and their Personal Information

SCA may possess records relating to Parents, Children, Staff, Board Members and Service providers etc.

Entity Type	Personal Information Processed
Parent / guardian	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; Credit check; bank details
Children	Names; contact details; physical and postal addresses; date of birth; ID number; nationality; gender; Record of School progress Confidential correspondence including Educational, health and psychological reports
Staff	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence including CV; qualifications; police clearance; sex register clearance; criminal record

	Banking details; record of earnings
Board Members	Names; contact details; physical and postal addresses; date of birth; ID number; nationality; gender; employment confidential correspondence including CV
Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories
Other	
Other	

5.3. Categories of Recipients for Processing the Personal Information

SCA may share the Personal Information with the appropriate staff, Board members as well as the following statuary bodies who may use this information to for record keeping and statistical purposes only:

Department of Education
Department of Social Development
Association of Christian Schools International
Other

SCA may supply the Personal Information to any party to whom SCA 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, organising and storing of data.
- Sending of emails and other correspondence to stakeholders.
- Conducting due diligence checks.
- Administration of the Medical Aid and Pension Schemes.
- Administration of Workman compensation
- Other

5.4. Actual or Planned Transborder Flows of Personal Information

Personal Information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws. SCA will endeavour to ensure that all service providers holding Personal Information relating to the school will make all reasonable efforts to secure said data and Personal Information.

5.5. Retention of Personal Information Records

SCA may retain Personal Information records permitted or required by law.

5.6. General Description of Information Security Measures

SCA will endeavour to employ up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

Digital Information

- Firewalls
- Virus protection software and update protocols
- Secure facilities for paper documents.
- Access control and passwords
- Secure setup of hardware and software making up the IT infrastructure;
- Outsourced Service Providers who process Personal Information on behalf of SCA are contracted to implement security controls.

Paper Documentation

- Secure filing cabinets
- Controls for accessing Personal Information

6. ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by SCA. Any requests should be directed, on the prescribed form, to the Information Officer.

6.1. Remedies available if request for access to Personal Information is refused

6.1.1. Internal Remedies

An individual or entity whose request has been refused by the School Information Officer may appeal, in writing to the School Board within 14 days. The decision of the School Board pertaining to a request is final.

6.1.2. External Remedies

A requestor that is dissatisfied with the information officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the information officer's decision to grant a request for information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

6.2. Grounds for Refusal

SCA may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which the School may refuse access include:

- Protecting personal information that the school holds about a Parent, Child, Staff and/or Board Member from unreasonable disclosure.
- Protecting commercial information that the school holds about a third party or supplier.
- If disclosure of the information would result in a breach of confidence owed to a third party in terms of an agreement.
- If disclosure of the record would endanger the life or physical safety of an individual.
- If disclosure of the record would prejudice or impair the security of property.
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme.
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived.
- Disclosure of the record would put the School at a disadvantage in contractual or other negotiations or prejudice it in commercial competition.

Records that cannot be found or do not exist:

If the School 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.

7. IMPLEMENTATION GUIDELINES

7.1. Training & Dissemination of Information

This Policy has been put in place throughout the School. Training on the Policy and POPI will take place with all affected employees and stakeholders.

All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPI.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

7.2. Employee Contracts

Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

Each employee currently employed within SCA will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

8. EIGHT PROCESSING CONDITIONS

POPI is implemented by abiding by eight processing conditions. SCA shall endeavour to abide by these principles in all its possessing activities.

8.1. Accountability

SCA shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. The School shall remain liable for compliance with these conditions, even if it has outsourced it processing activities.

- The School will confirm the appointment, in writing, of the School Information Officer.
- The School will register the Information Officer with the Regulator.
- The School Information Officer will acknowledge, in writing, the role and responsibility of this appointment.
- The School may appoint, in writing, a Deputy School Information Officer.
- The School will clarify, in writing, the roles and responsibility of the Deputy School Information Officer.

8.2. Processing Limitation

8.2.1. Lawful grounds

The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

SCA may only process Personal Information if one of the following grounds of lawful processing exists:

- The Data Subject consents to the processing.
- Processing is necessary for the conclusion or performance of a contract with the Data Subject.
- Processing complies with a legal responsibility imposed on the school.
- Processing protects a legitimate interest of the Data Subject.
- Processing is necessary for pursuance of a legitimate interest of SCHOOL, or a third party to whom the information is supplied;

Special Personal Information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Trade union membership;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour;
- Information concerning a child.

The School may only process Special Personal Information under the following circumstances:

- The Data Subject has consented to such processing and/or Parent (Legal Guardian) in the case of a minor child.
- The Special Personal Information was deliberately made public by the Data Subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons
- If processing of race or ethnic origin is in order to comply with affirmative action laws

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 processing then the School shall forthwith refrain from processing the Personal Information.

8.2.2. Collection directly from the Data Subject

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

- Personal Information is contained in a public record.
- Personal Information has been deliberately made public by the Data Subject.
- Personal Information is collected from another source with the Data Subject's consent.
- Collection of Personal Information from another source would not prejudice the Data Subject.
- Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the Data Subject would prejudice the lawful purpose of collection;
- Collection from the Data Subject is not reasonably practicable.

- The School will revise and update all documentation that requests Personal Data from individuals to ensure that the following is included:
  - Permission is being requested
  - Reasons for the collection of specific data is provided
  - Differentiation between Personal Data and Special Personal Data is clear with specific consent requirements included.
  - Parents will be informed and requested to consent to the collection of Personal Data from their children.
  - Revision of Personal Information required from an employee. (see POPI Manual)
- The School will ensure that all Personal Data collected digitally also contain the required consent and explanations. (as above)

8.3. Specific Duties and Responsibilities

8.3.1. Governing Body

The School Governing Body cannot delegate its accountability and is ultimately answerable for ensuring that the school meets its legal obligations in terms of POPIA. The Governing Body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

• The School appoints an Information Officer, and where necessary, a Deputy Information Officer.

• All persons responsible for the processing of personal information on behalf of the School:
  - are appropriately trained and supervised to do so,
  - understand that they are contractually obligated to protect the personal information they come into contact with, and are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

• Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

• The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the school holds, uses, shares, discloses, destroys and processes personal information.

8.3.2. Information Officer

The School's Information Officer is responsible for:

• Taking steps to ensure the school's reasonable compliance with the provision of PO PIA.

• Keeping the governing body updated about the school's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to PO PIA.

• Continually analysing privacy regulations and aligning them with the school's personal information processing

procedures. This will include reviewing the school's information protection procedures and related policies.
• Ensuring that PO PI Audits are scheduled and conducted on a regular basis.
• Ensuring that the school makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the school. For instance, maintaining a "contact us" facility on the organisation's website.
• 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. This will include overseeing the amendment of the school's employment contracts and other service level agreements.
• Encouraging compliance with the conditions required for the lawful processing of personal information.
• Ensuring 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 made by the school's data subjects.
• 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.
The Deputy Information Officer will assist the Information Officer in performing his or her duties.

8.3.3 IT

The School's Information Officer 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 shacking 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 electronically stored personal information has been accessed or acquired by any unauthorised persons.
• 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.

8.3.4. Marketing & Communication Administrators

The School's Marketing & Communication administrators are responsible for:
• Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the school's website, 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.
• Where necessary, working with persons acting on behalf of the school to ensure that any outsourced marketing initiatives comply with POPIA.

8.3.5 School Employees

School employees will, during the course of the performance of their services, gain access to and become acquainted with the personal information of parents, children, board members, other employees and suppliers.
School employees are required to treat personal information as a confidential school asset and to respect the privacy of data subjects.
School employees 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.
School employees must request assistance from the school management team or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.
School employees 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.
Furthermore, personal information will only be processed where the data subject:
• Clearly understands why and for what purpose his, her or its personal information is being collected; and
• Has granted the school with explicit written or verbally recorded consent to process his, her or its personal information.
School employees will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

- Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.
- Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.
- Consent to process a data subject's personal information will be obtained directly from the data subject, except where:
    - the personal information has been made public, or
    - where valid consent has been given to a third party, or
    - the information is necessary for effective law enforcement.

School employees and other persons acting on behalf of the organisation 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 smart phones. All personal information must be accessed and updated from the school's central database or a dedicated server.
• Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant school management team or the Information Officer.
• Transfer personal information outside of South Africa without the express permission from the Information Officer.
School 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 personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the school, with the sending or sharing of personal information to or with authorised external persons.
• 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 medias 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 subjects contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the school management team or the Information Officer to update the information accordingly.
• 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 school management team or the Information Officer to delete or dispose of the personal information in the appropriate manner.
• Undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the school, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

8.3. Purpose Specification
SCA must ensure that personal information is only processed for specific, explicitly defined and legitimate reasons relating to the functions or activities of the school and it must furthermore take steps to make the data subject (person whose personal information is being processed) aware of the purposes for which the personal information will be processed. Personal information may only be kept for as long as it is required to fulfil the purpose for which it was collected.

- Any Personal Data requested both in paper documentation and digitally will be reviewed to determine the necessity of that data. Any unnecessary data requests will be removed from the required fields.
- The School will provide legitimate written reasons and purposes for the requested Personal Data.
- The School will classify all Personal Information according to lawful retention and will ensure the lawful destruction of Personal Information after this time.
- The archiving of Personal Information for the required retention period will be done to ensure safety and security.

8.4. Further Processing
New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- Data Subject has consented to the further processing
- Personal Information is contained in a public record
- Personal Information has been deliberately made public by the Data Subject
- Further processing is necessary to maintain, comply with or exercise any law or legal right
- 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.

- SCA will obtain further consent from the Data Subject and/or Parent or Legal Guardian if Personal Information already obtained is required for further processing. Reasons for this request must be provided, indicating how the Personal Information will be used.

8.5. Information Quality

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

SCA should, as far as reasonably possible, follow the following guidance when collecting Personal Information:

- Personal Information should be dated when received;
- A record should be kept of where the Personal Information was obtained;
- Changed to information records should be dated;
- Irrelevant or unneeded Personal Information should be deleted or destroyed;
- Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

- The School will verify the identity of the Data Subject on collection of the Personal Information.
- The School will review the accuracy of individual Personal Information through annual updates. This will be done through an annual re-registration process that includes Personal Information. Any unneeded Personal Information should be deleted or destroyed.
- The school will implement a process whereby the Data Subject may update / change Personal Information either by paper document or on-line process.

8.6. Openness

SCA shall take reasonable steps to ensure that the Data Subject is made aware of:

- What Personal Information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection
- Whether the Personal Information shall be shared with any third party.

- The School will indicate on all documents where Personal Information is requested what the information will be used for.
- The School will communicate the rights of the individual to:
  - Access their personal Information
  - Lodge a complaint to the Regulator for suspected misuse of Personal Information.
- The School must clarify what personal information will be shared with 3rd parties:
  - Department of Education
  - ACSI
  - Other
- The School will obtain consent from the Data Subject or Parent / legal Guardian for the sharing of information to any 3rd party.

8.7. Data Subject Participation

The Data Subject have the right to request access to, amendment, or deletion of their Personal Information. All such requests must be submitted in writing to the Information Officer. Unless there are grounds for refusal as set out by the Act, the School shall disclose the requested Personal Information:

- On receipt of adequate proof of identity from the Data Subject, or requester
- Within a reasonable time
- On receipt of the prescribed fee, if any
- In a reasonable format

SCA shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

- SCA will communicate the process for any individual to have access to their Personal Information. This may be to make changes to Personal Information or to withdraw particular consent for processing Personal Information.
- **School Personal Information Request Form**.

8.8. Security Safeguards

SCA shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks;

8.8.1. 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 non-staff members may access them;
- SCA shall implement and maintain a "Clean Desk Policy" where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
- Personal Information which is no longer required should be disposed of by shredding.
- Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

8.8.2. Electronic Records

- 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.
- The School shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day.
- Electronical Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

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 notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

- The School undertake an annual risk assessment for the safe-guarding of Personal Information. An action plan will be carried out by the Information Officer to mitigate these risks.
- The School will ensure all personal documents are efficiently collated and stored in a secure facility.
- The document storage facility must have restricted access control. Records of access to Personal Information must be kept by the Information Officer of duly appointed person.
- All archived documents must be stored in a secure facility with controlled access. These documents must be destroyed after the legally required retention period.

- The School will conduct an annual **3rd Party Risk Assessment** to identify the Personal Information held and processed by these parties.
- The School will ensure that a contract exists with all 3rd party organisations to ensure the protection of Personal Information:
  - School Digital Administration software companies – EDUADMIN
  - SASAMS
  - Other
- IT will ensure the safe-guarding of Personal Information by implementing an IT policy for the protection of Personal Information in the School, including:
  - Server and personal computer firewalls
  - Regular monitoring and reporting of access to Personal Information
  - Password controls and computer locks.
  - Safe-guarding email sharing through bulk emailing.
- The School must communicate the process to be followed in case of a breach of security. (see POPI manual)
- CCTV footage is considered Personal Information. Recordings must be stored in a secure place with restricted access. All individuals must be informed about the existence and purpose of the CCTV cameras.

9. DIRECT MARKETING

All Direct Marketing communications shall contain SCA details, and an address or method for the parents / individuals to opt-out of receiving further marketing communications. Direct marketing in SCA includes:

- Newsletters
- Social media Platforms
- Communications via cell-phone technology (WhatsApp)

9.1. Existing stakeholders

Direct Marketing by electronic means to existing parents / partners/ people is only permitted:

- If the communication details were obtained on application to the school
- For the purpose of marketing / communicating similar newsletters.

The parent / supplier / person must be given the opportunity to opt-out of receiving direct communications on each occasion of direct marketing / communicating.

9.2. Consent

SCA may send electronic direct marketing communication to Data Subjects who have consented to receiving it. The School may approach a Data Subject for consent only once.

9.3. Record Keeping

SCA shall keep record of:

- Date of consent
- Wording of the consent
- Who obtained the consent
- Proof of opportunity to opt-out on each marketing contact
- Record of opt-outs

- The School will ensure and opt-out option on all marketing communications
- The School will obtain consent from Data Subjects and/or Parents / legal Guardian for the use of photos, video material etc for marketing purposes.

10. DESTRUCTION OF DOCUMENTS

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

10.2. The administrator in each section of the school is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order 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 School pending such return.
10.3. The documents must be destroyed by shredding.
10.4. Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

11. STATUTORY RETENTION PERIODS
The school will retain documents, records as follows:

Legislation	Document Types	Retention Perion
Companies Act	Record of Directors / Board members Minutes of Board Meetings Reports for AGM's Annual Financial Statements	7 years
Companies Act	Registration certificate NPO / PBO Certificates	Indefinitely
Consumer Protect Act	Application forms, parent contracts, financial records. Copies of progress reports	3 Years
Compensation for Occupational Injuries and Diseases Act	Register of all employees, earnings. Record of incidents reported at work	4 Years 3 years
Basic conditions of Employ Act	Written particulars of employer after termination.	3 years
Employment Equity Act	Record of Employment Equity plan.	3 Years
Labour Relations Act	Records of employee including disciplinary records.	3 years
Unemployment Insurance Act	Records of employees, remuneration etc	5 years
Income Tax Act	Employee tax records	5 years

12. STAFF TRAINING AND ACCEPTANCE OF RESPONSIBILITIES

12.1 Training.
SCA will ensure that on-going and regular staff and stakeholder training take place, including the following:
- Understanding of the POPI Act and the implementation thereof
- Application of the School POPI policy and procedures
- Role and responsibility of Information Officer and all staff handling Personal Information.

12.2 Responsibility
SCA Works Information Officer will ensure that all staff who have access to any kind of personal information will have their responsibilities outlined.
All staff will sign a confidentiality and responsibility clause in their employment contract as well as an acceptance of the School POPI policy and Procedure document.

13. POPI COMPLAINTS PROCEDURE
Data Subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The School will take all complaints seriously and will address all complaints in accordance with the following procedure:

13.1. All POPI complaints must be submitted to the School Information Officer on the required POPI Complaint Form either on paper which must be delivered to the school or digital in the form of an email.
13.2. The School Information Officer must acknowledge receipt of the complaint within 2 working days.
13.3. The School Information Officer will consider the complaint and efficiently conduct any research appropriate to the complaint. The School Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles of POPIA.
13.4. The School Information Officer must record his/her findings of the complaint and must respond to the complainant in writing as soon as reasonably possible.
13.5. Where the School Information Officer has reason to believe that Personal Information of data subjects has been accessed or acquired by an unauthorised person, he/she will inform:
- the School Governing Body
- the affected Data Subjects
- the Information Regulator

13.6. The response to the complainant may include the following:
- a suggested remedy or redress for the complaint
- a dismissal of the complaint with reasons provided
- a written apology (if applicable) and any disciplinary action that may be taken against the responsible person/s.

13.7. Where the complainant is not satisfied with the solutions to the complaint, the complainant has the right to complain to the Information Regulator.

14. DISCIPLINARY ACTION

Where a POPI complaint or infringement investigation has been finalised, SCA may recommend any appropriate administrative, legal and/or disciplinary action to be taken against an employee reasonably suspected for being implicated in any non-compliant activity outlined within this policy.

14.1. In case of ignorance or minor negligence, the school will undertake to provide further awareness training.
14.2. In case of gross negligence or wilful mismanagement of Personal Information, the school may proceed with disciplinary action.

15. POLICY REVIEW AND REPORTING

15.1 The School Information Officer is responsible for an annual review to be completed prior to the policy anniversary date. The Information Officer will ensure relevant stakeholders are consulted as part of the annual review to be completed.
15.2 The School Information Officer will review the RISK Analysis on an annual basis. A strategic plan will be developed to address the needs. The POPI Policy and Procedure document will be updated as required.
15.3 The School Information Officer will submit all reports as required by the Information Regulator.