THE SETTLERS HIGH SCHOOL

POLICY MANUAL FOR THE

PROTECTION OF PERSONAL INFORMATION

AND THE RETENTION OF DOCUMENTS AND RECORDS

IN TERMS OF THE POPIA

NAME OF THE POLICY:
THE SETTLERS HIGH SCHOOL POLICY MANUAL FOR THE PROTECTION OF PERSONAL INFORMATION AND THE RETENTION OF DOCUMENTS AND RECORDS IN TERMS OF THE POPIA.

SHORT NAME OF POLICY:
TSHS POPIA POLICY

EFFECTIVE DATE:
1 JULY 2021

DATE OF NEXT REVIEW:
TO BE CONFIRMED

REVISION HISTORY:
NO REVISIONS HAVE BEEN MADE AS YET

FREQUENCY OF REVIEW:
EVERY SGB CYCLE OR AS NEEDED

TABLE OF CONTENTS

1. PREAMBLE

1.1 The Settlers High School is a public school in terms of the South African Schools Act 84 of 1996 (as amended) and is managed and governed in terms of the provisions of the act as well as the language and admissions policy drafted in terms thereof. The medium of instruction at the school is English. The school offers education in Grades 8 to 12.

1.2 A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions. Given the importance of privacy, the school is committed to effectively managing personal information in accordance with POPIA's provisions.

1.3 POPIA establishes the rights and duties designed to safeguard the personal data of an individual. In terms of the act, the legitimate needs of the school to collect and use personal data for its business and other purposes are balanced against the right of data subjects to have their right of privacy, in the form of their personal details, respected.

1.4 POPIA is not intended to prevent the processing of personal information, but rather to ensure that it is done fairly and without adversely affecting the rights of data subjects. Given the wide-ranging impact of the POPIA, it is expressly provided that all collecting, storing, and processing of personal information must conform to the POPIA's provisions.

1.5 The school regards the lawful and appropriate collecting, storage, and processing of all data such as Personal Information as crucial to successful service delivery and essential to maintaining confidence between the school and those persons (also known as "data subjects" in terms of POPIA) and entities/agencies/businesses/persons who deal with the school. The school therefore fully endorses and adheres to the principles of the Protection of Personal Information Act, Act 4 of 2013 (POPIA) and the regulations promulgated in terms of the Act.

1.6 Therefore, it is critical that all staff of the school work to the highest attainable standards with regard to this Policy Manual and the prescripts of POPIA and other related legislation and policies. The school's integrity includes both the way in which staff conduct themselves and the way in which all ensure the data the school hold is compliant with relevant legislation.

1.7 Postal address of the school:

The Settlers High School
PO Box 599
Bellville
7535
South Africa

1.8 Street address of the school:

The Settlers High School
Settlers Street
Bellville
7530
South Africa

1.9 Telephone number of the school:
+27(21) 948 – 6116

1.10 E-mail address of the school:
info@settlers.org.za

1.11 The Information Officer is the school principal, currently, Mrs S Gallie.
Her e-mail address is: principal@settlers.org.za

1.12 The Deputy Information Officers are Mr GHI Nieuwoudt and Ms B Dyck.
Their e-mail addresses are: ng@settlers.org.za and db@settlers.org.za respectively.

2. OBJECTIVES OF THE POLICY MANUAL

2.1 To safeguard the personal information held by the school from threats, whether internally or externally, deliberate, or accidental and thus protecting the right of privacy of all data subjects as listed in Annexure A of this policy.

2.2 Protecting the school's records and information as listed in Annexure A to ensure the continuation of the day to day running of the school.

2.3 Regulating the manner in which personal information is collected, stored and processed by the school and stipulates the purpose for which information collected is used.

2.4 Appointing Information Officers to ensure respect for and to promote, enforce and fulfil the rights of data subjects referred to in Annexure A.

2.5 To protect the school from the compliance risks associated with the protection of personal information which includes:

a. Breaches of confidentiality where the school could suffer loss in revenue where it is found that the personal information of data subjects have been shared or disclosed inappropriately.

b. Failing to offer a choice, including the choice where all data subjects should be free to decide how and for what purpose the school may use information relating to them.

c. Any instances of any reputational damage where the school could suffer a decline in its reputation, or its good name is impugned through the actions of another party who disseminates or has gained unauthorised access to any personal information of the school's data subjects.

3. DEFINITIONS/TERMINOLOGY AND ACRONYMS

3.1 Definitions

Term	Explanation
Accessibility of data	The ease with which data can be obtained.
Accuracy of data	The degree to which the output correctly describes the data.
Acting at Arms' Length	Means acting independently (i.e. without outside influence).
Administrative data	Data collected from administrative sources.
Advanced Electronic Signature	Means an electronic signature which results from a process which has been accredited by an Authority as provided for in section 37 of ECTA.
Anonymisation	Is a process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly.
Archive	Means a repository holding physical documents/files and/ or other material containing a variety of data, it can also be data in an electronic format and/or in the Cloud. (Also see document).
Authentic records/documents/information	Authentic records are records that can be proven to be what they purport to be. They are also records that are considered by the creators to be their official record.
Authoritative records/Information/document	Authoritative records/information are records that are authentic, reliable, trustworthy, and useable and are complete and unaltered.
Automated	Refers to using equipment that processes information automatically according to a data processor's instructions.
Automated Transaction	Means an electronic transaction conducted or performed, in whole or in part, by means of electronic data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment.
Best interests of the child	The best interests of the child should be the primary consideration when a child's information is processed or it is considered to legally disclose such information to a third party, a natural or other person.
Biometrics	Means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
Bots/Chatbots	Bots are automated electronic software programmes that run over the Internet. Chatbots and social bots are programmed to mimic natural human interactions such as liking, commenting, following, and unfollowing on social media platforms.
Browser	Means a computer programme which allows a person to read hyperlinked data messages or access such messages on the internet via a search engine on an electronic device.
Child	Means a natural person under the age of 18 years who is **not legally competent**, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.
Certified Copy [of a document]	A "certified copy" is a copy of an official primary document that has on it an endorsement or certificate that it is a true copy of the primary document. A certified copy does not certify that the primary document is genuine, only that it is a true copy of the primary document.
Circuit Manager	The head of an education circuit of the WCED in the particular District to which the school has been assigned for administrative/managerial purposes.
Competent Person	Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child. [Also see *In loco parentis*]

Term	Explanation
Confidential Information	a. Confidential Information is a broader category than personal information. b. This means that as a general rule, all personal information is confidential and should be kept confidential, but not all confidential information is necessarily personal information. c. The school's business plan, strategic plans, development plans, financial records and whole school evaluation may be regarded as confidential without containing personal information. d. Confidential means to be entrusted with another person's confidence or secret affairs.
Consent	Consent by and of and for the data subject [by parents and guardians of learners and other legally authorised agents/representatives] means any freely [voluntarily] given, specific, informed expression of will and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, and/or signature including an electronic signature or any other electronic and/or written method, signifies agreement to the processing of personal data relating to him or her in terms of POPIA, this policy and related policies and legislation.
Constitution	Means the Constitution of the Republic of South Africa, 1996, as amended.
COVID-19	COVID-19, also known as the Coronavirus, is an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) that was declared a pandemic by the World Health Organization on 11 March 2020.
Custody of records/documents	The control of records/documents based upon their physical possession.
Data	Means electronic representations of information in any form.
Data breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Data confidentiality	A collection of data indicating the extent to which its unauthorised disclosure could be prejudicial or harmful to the interest of the source or other relevant parties.
Data credibility	The quality, capability, or power of the data to elicit belief that it is true.
Data Message	Means information generated, sent, received or stored by any electronic means well as the definition in section 1 in ECTA and other legislation i.e. any electronic representations of information in any form as well as a stored record and voice message/recording.
Data Subject	Means any natural person /juristic person to whom any information relates to and who provides the requested information by his/her own expression of will [and on behalf of any minor in case of a parent/guardian/care giver to the school.
De-Identify	De-identify", in relation to personal information of a data subject, means to delete any information that - a) identifies the data subject; b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and "de-identified" has a corresponding meaning.
Deputy Principal	An educator appointed to the post and assigned duties to assist the principal and to deputise for the principal during his/her absence.
Disposal	The action of either destroying/deleting a record/ document/personal information or transferring it into archival custody.

Term	Explanation
Direct Marketing	Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; and/or b) requesting the data subject to make a donation provide sponsorship of any kind for any reason.
[Education] District Office	Means the District Office of the GDE in the educational district in which the school is located.
District Director/Manager	Means the officer of the department responsible for the administration of education in a particular educational district.
Document	Means any book, map, pamphlet, letter, circular letter, list, record, placard, poster, notice, pdf electronic document, [any] electronic information or any other document stored on a data base of a server/computer/electronic handheld device, web page, blog, App and also printed and electronic newspapers, magazines, periodicals, blogs, and everything that contains the written pictorial proof of something and it does not matter what the material is made of.
Domain Name	Means an alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet.
Domain Name System	Means a system to translate domain names into IP addresses or other information.
Education	Education undertaken in an educational Institution established, declared, or registered in terms of the South African Schools Act and the relevant provincial education act.
Education Management	The day-to-day organisation of teaching and teaming, and the activities that support teaching and learning. The professional management of the school is the responsibility of the principal who is also the manager of the school and other members of the school management team. Management in the school includes a wide variety of processes related to teaching and learning and including the collection and management of data and information.
Education Management Information System (EMIS)	A system designed to systematically organise Information related to the management of educational development in education in the school and the DBE
Educator	Means any person, excluding a person who is appointed to exclusively perform extracurricular duties, who teaches, educates, or trains other persons or who provides professional educational services, including professional therapy and education psychological services, at the school.
Electronic Communication	Means any text, voice, sound, video, photograph, payment transaction or image message sent over an electronic communications network using a computer/electronic handheld device/tablet/cell phone/Wi-Fi/Smart phone/smart watch which is stored in the network or in/on the recipient's terminal /handheld/portable/digital/electronic equipment until it is collected/accessed by the recipient and is available on any social media platform or App and include any other electronic communication posted or forwarded to another person's device/computer/tablet/cell phone/Wi-Fi/Smart phone/smart watch.
Electronic records	Information/data which is generated electronically and stored by means of computer/electronic/digital technology. Electronic records can consist of an electronic correspondence system and electronic record systems other than the correspondence system.

Term	Explanation
Electronic Signature	Refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user/person/applicant/data subject/third party to serve as a signature. Examples of electronic signatures include: a) the school typed name at the end of the school e-mail, b) a scanned image of the school handwritten signature embedded into a Word document; and c) a so-called digital signature. ECTA also creates special type of electronic signature, known as an "advanced electronic signature".
Electronic records/data/ Information system	This is the collective noun for all components of an electronic information system, namely: electronic media as well as all connected items such as source documents, output information, software applications, programmes and meta data (background and technical information i.r.o. the information stored electronically) and in hard copy. All these components are defined as records/documents/information in terms of this policy.
Electronic Transactions/ Electronic Financial Transaction/Payments	Include e-mails sent and received, other messages sent and received on any electronic/digital messaging platform, properly authorised payments made and received by EFT and to the credit of the school's bank account and from the school's account to another party's account using any social media platform/ banking App/ATM.
E-mail	Means electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication or that can be forwarded to another person and to which other documents can be attached.
Enrolled learner	A learner who is admitted at the school and whose name is recorded in the admission register.
Expression of Will	Means that a data subject must indicate, in some manner that he/she agrees to supply legally requested information to the school orally or in writing.
File Plan	A pre-determined classification plan by which records/documents/information are filed and/or electronically indexed to facilitate efficient retrieval and disposal of records.
Filing System	a. POPIA only applies to the processing of personal information which is in a record which forms part of a filing system. b. A filing system therefor means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria and/or accessed using in any digital electronic format by means of any the recipient's computer terminal/handheld/portable digital/electronic equipment or in hard copy/Written format. c. The collective noun for a storage system (like files, boxes, shelves or electronic applications and storage systems) in which records are stored in a systematic manner according to a file plan.
[School] Governing Body	Means the governing body of the school as contemplated in section 16 (1) of SASA.
Historical data	Refers to data that is two or more years old.
Home Page/Web Site	Means the primary entry point of a web page of a web site on the internet of a person or natural person.
Hyperlink	Means a reference or link from some point in one data message directing a browser or other technology or functionality to another data message or point therein or to another place in the same data message.
Information	Data presented in a context so that it can be applied or used.

Term	Explanation
Information Matching programme	a) An information matching programme is the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information regarding ten or more data subjects, with one or more other documents that contain personal information of each of those ten or more data subjects. b) The purpose of the information matching programme is to produce or verify information that may be used to take action regarding any of those data subjects.
Information Officer	Information officer of, and/or in relation to, the school means the information officer or deputy information officer as contemplated in terms of section 1 or 17 of POPIA. The Information Officer is responsible for ensuring the school's compliance with POPIA. Where no Information Officer is appointed, the principal of the school will be responsible for performing the Information Officer's duties. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
[Information]Regulator	Means the Information Regulator established in terms of section 39 of POPIA.
Informed	Means the data subject are properly informed what information he/she consents to supplying to as requested by the school to be processed by an operator and requested to read the document requesting the information and indicate that he/she has read it and understands it.
In Loco Parentis	Means acting in the place of a parent who has entrusted the custody and control of his or her child to an educator or another person during normal intramural or extramural school activities.
Judgment	A decision by a court that resolves a dispute and determines the right and obligations of the parties. Judgments also generally provide the court's explanation of why it has chosen to make a particular court order.
Juristic Person	Includes a partnership, close corporation, company or other bodies such as the school represented by the SGB.
Learner	Means any person receiving education or obliged to receive education at the school in terms of SASA.
Learner profile	A continuous record of information that provides an all-round impression of a learner's progress, behavioural record, including the holistic development of values, attitudes, and social development.
Member of the Executive Council	Refers to the Member of the Executive Council for Education in the Western Cape Province.
Member of Staff/Staff Member	Means a person employed at the school.
Mobile Social Media	Mobile social media refer to the use of social media on mobile devices such as cell phones/smartphones, smart watches and tablet computers.
Operator	Means a person who processes personal information/data collected for and on behalf of the school (internal or external) in terms of a contract, employment contract, or a mandate without coming under the direct authority of the school and do not use the data for personal purposes.
Parent/Guardian/Caregiver	Means- (a) the biological or adoptive parent or legal guardian of a learner; (b) the person legally entitled to custody of a learner; or (c) the person who undertakes to fulfil the obligations of a person referred to in paragraphs (a) and (b) towards the learner's education at the school.
Person	Means a natural person or a juristic person.

Term	Explanation
Personal Information	Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; b) information relating to the education or the medical, financial, criminal or employment history of the person; c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; d) the biometric information of the person; e) the personal opinions, views or preferences of the person; f) Correspondence [including any electronic correspondence] sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; g) the views or opinions of another individual about the person; and h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
Personal Identifiable Information/Online Identifier	Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier/online identifier such as an IP address/"cookies"/identifier on a mobile phone/landline phone.
Policy Manual	Means this Privacy and Protection of Personal Information Policy Manual of the school.
Prescribed	Means prescribed by regulation or by a code of conduct in terms of POPIA.
Principal	Means an educator appointed or acting as the head of the school.
Private Body	Means: a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; b) a partnership which carries or has carried on any trade, business, or profession; or c) any former or existing juristic person, but excludes a public body such as the school.
Privilege	Means the right claimed by a person to refuse or divulge information of another obtained in confidence from another.
Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: a. the collection, receipt, recording, organisation, collation, storage, updating or modification, amending, adapting, handling, storing retrieval, alteration, consultation or use; b. dissemination/disclosing by means of transmission, distribution or making available in any other form; or c. merging, linking, as well as restriction, degradation, erasure, or destruction of information. d. aligning, combining, blocking, erasing, or destroying the data.
Professional Legal Adviser	Means any legally qualified person/legal firm contracted by the school, whether in private practice or not, who lawfully provides the school or a client, at the school's request or the client's request, with independent, confidential legal advice.
Protection of Personal Information Act	Is a law passed by the South African Parliament, which sets the conditions that the school must follow to lawfully process the personal information about persons.

Term	Explanation
Public Body [Including the School]	means— a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or b) any other functionary or institution when - i. exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or ii. exercising a public power or performing a public function in terms of any legislation.
Public record	A record created or received by a governmental body and the school in pursuance of its activities, regardless of form or medium.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Public Record	Means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
Recipient	Means a natural or legal person, public authority, agency, or another body, to which the personal data are legally disclosed in any format, whether a third party or not.
Record	Means any recorded information - a) regardless of form or medium, including any of the following: i. Writing on any material; ii. information produced, recorded or stored by means of any tape recorder, sound recording, computer equipment, mobile phone, closed circuit camera, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; iii. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; iv. in a book and/or as a map, plan, graph or drawing; v. photograph, film, video (digitally or electronically), negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced in any form or in any software programme; b) in the possession or under the control of the school; c) whether or not it was created by any responsible party; and d) regardless of when it came into existence.
Recording	Anything on which sounds or images or both are fixed, or from which sounds or images or both are capable of being reproduced, regardless of form.
Regulator	Means the Information Regulator established in terms of section 39 of POPIA.
Re-identify	In relation to personal information of a data subject, means to resurrect any information that has been de-identified, that - a) identifies the data subject; b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or c) can be linked by a reasonably foreseeable method to other information that identifies the data subject; and d) re-identified has a corresponding meaning.

Term	Explanation
Representative	Means in the context of this policy manual, a natural or legal person established in the Republic of South Africa designated by a public or private body or even the school who are legally entitled to provide information on any data subject to the school and who are entitled to sign any legal document/letter/email/ correspondence or other legal instrument on behalf and for such natural or legal person.
Responsible Party	Means a public or private body such as the school as a juristic person or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
Restriction	Means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.
Retention Period	The length of time that records should be retained in offices before they are either transferred into archival custody or destroyed/deleted.
Scanned Document/Document Scanning	Document scanning in context of this policy means the process of capturing paper documents and converting them to a digital format via a document scanner or multi-function printer. Document scanning is also commonly referred to as document conversion or document imaging.
School	Means, The Settlers High School a public school which enrols learners in one or more grades from grade 8 to grade 12.
School Activity	Means any official educational, cultural, recreational, or social activity of the school within or outside the school premises.
School Fees	Means school fees contemplated in section 39 of SASA and includes any form of contribution of a monetary nature made or paid by a person or body in relation to the attendance or participation by a learner in any programme of the school.
Sensitive Data	See Special Personal information.
Sibling	Means someone who satisfied both the following requirements: a) He or she has a parent who is also the parent of that child; and b) He or she resides in the same household as that child.
Signature	Includes an electronic signature as defined in section 1 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002). It also refers to the stylistic representation of a person's name, surname and/or initials that is applied to any document. The signature must be placed by the signatory him/herself and the signatory must have intended to sign the relevant document. A signature also includes an identical reproduction stamp of the original signature of the person who has instructed a person to stamp a document with his/her signature.
Social Media Platforms/Sites/Apps	Forms of electronic communication (such as websites/Apps for social networking, messaging, and microblogging) through which users create online communities/groups/chat groups to share/post information, chats, ideas, personal messages, and other content.
Social Media Services	Users usually access social media services via web-based apps on desktops and laptops, or download services that offer social media functionality to their mobile devices (e.g., smartphones and tablets). As users engage with these electronic services, they create highly interactive social media platforms through which individuals, communities, and organisations can post, create, share, co-create, discuss, participate and modify user-generated content or self-curated content posted online with the intent to share information, ideas, personal messages, and other content to other online users and/or followers/"friends"/receivers.

Term	Explanation
Special Personal Information	Means personal information as referred to in section 26 of POPIA. This includes all information relating to a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, or criminal behaviour. POPIA also specifically regulates personal information (of a child).
Specific	Refers to the precise and detailed legally information requested from a data subject and being clear about the purpose for which information is requested and processed.
Submit	Means submit by- a) data message; b) any form of an electronic communication on any app/social media platform provided the receiver is informed that such a message has been sent/posted; c) telephone of which there is a record; d) registered post; e) electronic mail including registered e-mail; f) facsimile; and g) personal delivery and/or by hand by any person.
Surveillance Cameras [CCTV]	Surveillance Cameras or Closed-Circuit Television Cameras (CCTV) are used by the school in monitoring the movements and behaviour of individuals; this can include video, audio, or live footage. For the purpose of this policy only video and audio footage or both, will be applicable. This will be clearly signposted at school property entrances and in the CCTV Policy of the school.
Third Party	Means a natural or legal person, public authority, agency, entity or body other than the data subject, parents of learners of the school, and persons who, under the direct authority of the school are authorised to process personal data.
Unique Identifier	Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.
User-generated Content	User-generated means electronic/digital content such as text posts or comments, digital photos or videos, and data generated through all online interactions using/posting generating content on any social media platform.
Voluntarily	Means that a data subject cannot be forced or pressured into giving consent except where the school is allowed legally to do so without his/her consent.
Web Page	Means a data message on the World Wide Web.
Web Site	Means any location on the Internet containing a home page or web page.
'World Wide Web' [www]	Means an information browsing framework that allows a user to locate and access information stored on a remote computer/handheld electronic device and to follow references from one computer/handheld electronic device to related information on another computer/hand held electronic device.
Writing	Includes writing as referred to in section 12 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002*): "12. A requirement in law that a document or information must be in writing is met if the document or information is-* *(a) in the form of a data message; and* *(b) accessible in a manner usable for subsequent reference."*

3.2 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
IO	Information Officer
DIO	Deputy Information Officer
IOP	Information Operator
MEC	Member of the Executive Council for Education in the Gauteng Province.
NAPTOSA	National Professional Teachers' Organisation of South Africa
PAIA	Promotion of Access to Information Act
POPI	Protection of Personal Information
POPIA	Protection of Personal Information Act, 2013
PII	Personally Identifiable Information
PSA	Public Service Association
SADTU	South African Democratic Teachers' Union
SAOU	Suid-Afrikaanse Onderwysers Unie
SASA	South African Schools Act, 1996
SBST	School Based Support Team
SGB	School Governing Body
SMT / EXCO	School Management Team / Executive Committee
TSHS	The Settlers High School
UGC	User-generated Content on any social media platform and/or using and posting data/information on any social media platform.
WCED	Western Cape Education Department

4. APPLICATION AND SCOPE OF THE POLICY

4.1 The Settlers High School is committed to protecting the privacy of data subjects and to ensure that their personal information is collected and used properly, lawfully and transparently.

4.2 The SGB and the Principal of the school are ultimately responsible for ensuring that information security is properly managed. The Information Officer, Ms S Gallie, is responsible for:

a. The development and upkeep of this policy.
b. Ensuring this policy is supported by appropriate documentation, such as procedural instructions.
c. Ensuring that documentation is relevant and kept up to date.
d. Ensuring this policy and subsequent updates are communicated to the SGB, staff and parents where applicable.
e. The SGB, the school's employees, volunteers, contractors, suppliers, and any other persons acting on behalf of the school are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
f. Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities of their particular areas of responsibility overseen by the information officers of the school.

4.3 This Policy Manual applies to all staff of the school, both permanent and temporary staff, to staff working on a contract basis for the school, coaches, volunteers, and others who are authorised to access personal data held by the school. The provisions of the policy are applicable to both on and off-site processing of personal information. Non-compliance with this policy may result in disciplinary action and possible termination of employment or mandate, where applicable.

4.4 All staff are responsible for reporting any security breaches or incidents to the Information Officer and/or Deputy Information Officers.

4.5 This policy applies to personal information collected, stored, and processed by the school in connection with the services it offers. This includes information collected offline, through the school's telephone lines, online through the school's websites, branded pages on third party platforms, and applications accessed or used through such websites or third-party platforms which are operated by or on behalf of the school. This policy is hereby incorporated into and forms part of the terms and conditions of use of the applicable school web sites and other social media platforms.

4.6 Line managers within the school are required to ensure that all staff who manage or have access to personal data comply with this Policy Manual. The SGB and Members of the SMT/EXCO are required to review procedures in their areas to ensure compliance with this Policy Manual and POPIA as part of the annual Business Planning process of the school.

4.7 This policy does not apply to:

a. information collected by third party websites, platforms and/or applications ("Third Party Sites") which the school/SGB/SMT/EXCO does not control;
b. information collected by Third Party Sites which a person can access via links on school sites; or
c. banners, competitions and other advertisements, services or promotions on Third Party Sites that the school may sponsor or participate in or just host advertisements for.
d. Information for purely household activities;
e. Information which has been de-identified;
f. Information which has been processed by or on behalf of another public body for the purposes of:
    i. Safeguarding national security;
    ii. The investigation and prosecution of criminal matters;
    iii. Processed by the Cabinet and its Committees or the Executive Council of a province;
    iv. Relating to the judicial functions of a court.
g. The processing of personal information for the purposes of journalistic expression in defined circumstances. The exclusion requires the journalist to be subject to a Code of Ethics and provides adequate safeguards for the protection of personal information.

It is important to note that the exclusions referred to above related to the processing by or on behalf of a public body for the purposes of national security and investigation of a crime are only granted to the State if adequate safeguards have been established in the legislation permitting the process of such information.

4.8 This policy impacts upon the school's work practices and data collection, storage, and processing for all those who:

a. create records including electronic records;
b. have access to records;
c. have any other responsibilities for records, for example storage and maintenance responsibilities;
d. have a management responsibility for staff engaged in any the activities as stipulated in the policy.

5. LEGISLATIVE FRAMEWORK

5.1 Constitution of the Republic of South Africa, Act 108 of 1996.
5.2 South African Schools Act, Act 84 of 1996.
5.3 National Regulations for Safety Measures at Schools, GN 1040 of 2001, as amended.
5.4 The Protection of Personal Information Act no 4 of 2013, as amended.
5.5 South African Council of Educators Act, 2000(Act No. 31 of 2000), as amended.
5.6 Public Service Act, 1994, as amended.
5.7 General Notice 6903 of 2000 as amended, Misconduct of Learners at Public Schools and Disciplinary Proceedings.
5.8 General Notice1040 of 12 October 200, as amended, Regulations for Safety Measures at Public Schools.
5.9 National Health Act, 2003 (Act No 61 of 2003), as amended and related regulations.
5.10 School Education Act, 1995 (Act 6 of 1995), as amended.
5.11 General Notice 1189 of 2012, Regulations on Domestic and International Tours for Learners at Public Schools, 2012.
5.12 Electronic Communications and Transactions Act, 25 of 2002.
5.13 Financial Intelligence Centre Act, Act 38 of 2001, as amended.
5.14 Compensation for Occupational Injuries and Diseases Act, Act 130 of 1993, as amended.
5.15 Basic Conditions of Employment Act, Act 75 of 1997.
5.16 Employment Equity Act, Act 55 of 1998.
5.17 Labour Relations Act, Act 66 of 1995 and Codes of Good Practice.
5.18 Unemployment Insurance Act, Act 63 of 2002.
5.19 Tax Administration Act, Act 28 of 2011.
5.20 Income Tax Act, Act 58 of 1962.
5.21 Skills Development Levies Act, Act 9 of 1999.
5.22 Securities Services Act, Act 36 of 2004.
5.23 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").
5.24 General and Further Education and Training Quality Assurance Act.
5.25 Regulations pertaining to POPIA.
5.26 Umalusi Policy and Criteria.
5.27 National Archives and Records Service of South Africa Act, (Act No 43 of 1996), as amended.
5.28 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.
5.29 National Education Policy Act, 1996, Act 27 of 1996, as amended.
5.30 The Criminal Procedure Act, Act 51 of 1977.
5.31 The Films and Publications Act, Act 65 of 1996, as amended.
5.32 Employment of Educators Act, 1998, Act 76 of 1998, as amended.
5.33 Regulation of Interception of Communications and Provision of Communication-Related Information Act, Act 70 of 2002.
5.34 Government Notice 487 dated 6 June 2011 - SC006: Dictionary of Education Concepts and Terms published by the Minister of Basic Education.
5.35 Copyright Act, Act 98 of 1978.
5.36 Short Term Insurance Act, Act 53 of 1998.

6. RELEVANT POLICIES AND PROVINCIAL CIRCULARS

6.1 School Health and Safety Policy.
6.2 Admission Policy of the School.
6.3 Language Policy of the School.
6.4 Religion Policy of the School.
6.5 Code of Conduct for Learners and related rules and policies of the School.
6.6 Extra Mural and Sports Policy of the School.
6.7 Asset Register of the School.
6.8 COVID-19 Protocol and Anti-Stigmatisation Policy of the School.
6.9 HIV/AIDS, TB and STIs Policy of the School.
6.10 Privacy Policy of the School.
6.11 School Social Media Policy.
6.12 School CCTV Policy.
6.13 Code of Conduct for Parents and Visitors of the School.
6.14 Personnel Administrative Measures.
6.15 SACE Code of Conduct and the Code of Conduct for public Servants.
6.16 Contractual obligations of employees employed by the SGB.
6.17 WCED Memorandum – Requirements for Storage of Examination Materials at the District Offices and Examination Centres - 2014

7. POLICY STATEMENTS

7.1 Key Principles of the Policy Manual

7.1.1 Unfortunately, POPI is not an event, in essence it requires a change in school culture with regard to information management and a concerted and directed effort. POPIA compliance requires at least the following:

a. Will from management.
b. Training of staff.
c. Regular inspection and information process flow management
d. Reporting and measurement of information management and processing.
e. Regular training and re-training of staff.

7.2 Commitment to the Principles of POPIA

7.2.1 The Information Officer, any authorised operator, and staff of the school is committed to the following principles:

a. To be transparent with regards to the standard operating procedures governing the collection and processing of personal information.
b. To comply with all applicable regulatory requirements regarding the collection and processing of personal information.
c. To collect personal information only by lawful and fair means and to process personal information in a manner compatible with the purpose for which it was collected.
d. Where required by regulatory provisions, to inform individuals when personal information is collected about them.
e. To treat special personal information that is collected or processed with the highest of care as prescribed by regulation.
f. Where required by regulatory provisions or guidelines, to obtain individuals' consent to process their personal information.
g. To strive to keep personal information accurate, complete and up to date and reliable for their intended use.
h. To develop reasonable security safeguards against risks such as loss, unauthorised access, destruction, use, amendment or disclosure of personal information.
i. To provide data subjects with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or delete personal information.
j. To share personal information, such as permitting access, transmission or publication, with third parties only with a reasonable assurance that the recipient has suitable privacy and security protection controls in place regarding personal information and are allowed to such access.
k. To comply with any restriction and/or requirement that applies to the transfer of personal information nationally and/or internationally.
l. All new employees of the school will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPIA.

7.3 The School is a Public Body

a. Exercising a power or performing a duty in terms of the Constitution of South Africa and a provincial constitution.
b. Performing and exercising a public power and performing a public function in terms of legislation.

7.4 The Principles of Compliance

a. Obtain consent before collecting data (or processing, storing, or sharing it).
b. Be sure to only collect data needed for legitimate purposes.
c. To use the information in a way that matches the purpose of collection.
d. Take reasonable security steps to protect the integrity of the information.
e. Store the information only as long as required.
f. Uphold data subjects' rights by providing access and corrections to information.

7.5 The School's Compliance Management System

7.5.1 Compliance is not a "one-and-done event". It is an ongoing and active process that requires management. The school should have an active compliance plan in place that provides for a systematic way to review and update the school's processing standards on a regular basis. The current active compliance plan includes regular review by the school's SMT/EXCO and at SGB meetings when needed.

7.6 Drafting New Policies and Update Existing Documents

7.6.1 POPIA requires the school to update existing policies and create new ones. The school has to have documents such as:

a. A Privacy Policy.
b. Information Security Procedures (included in this Policy).
c. Incident Response Policy for data breaches or any other matters related to personal data (included in this Policy).

7.6.2 The school must also share these policies with the school staff and third-party partners so that everyone knows what to do to comply with POPIA.

7.7 Rights of Data Subjects

7.7.1 Where appropriate, the school will ensure that all data subjects are made aware of the rights **conferred** upon them in terms of section 5 of POPIA. When a minor turns 18, the rights belong directly to him or her, unless it is stipulated to the contrary in other legislation.

7.7.2 The rights are as follows:

7.7.2.1 to be notified that personal information about him, her or it is being collected as provided for in terms of section 18 of POPIA or his, her or it's personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22 of POPIA;

7.7.2.2 to establish whether a responsible party holds personal information of that data subject and to request access to his, her or it's personal information as provided for in terms of section 23 of POPIA;

7.7.2.3 to request, where necessary, the correction, destruction or deletion of his, her or it's personal information as provided for in terms of section 24 of POPIA;

7.7.2.4 to object, on reasonable grounds relating to his, her or it's particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)(a) of POPIA;

7.7.2.5 to object to the processing of his, her or it's personal information at any time for purposes of direct marketing in terms of section 11(3)(b)of POPIA; or o object to the processing of his, her or its personal information at any time for purposes of direct marketing in terms of section 11(3)(b) of POPIA or in terms of section 69(3)(c) of POPIA;

7.7.2.6 not to have his, her or it's personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1) of POPIA;

7.7.2.7 not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71 of POPIA;

7.7.2.8 to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74 of POPIA; and

7.7.2.9 to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99 of POPIA.

7.8 A Word of caution to Parents/Guardians/Care Givers

7.8.1 While laws apply to what the school and third parties can disclose about learners, they do not apply to what learners or their parents might disclose publicly themselves This means the parent and the child also have a responsibility to protect their privacy. What a parent and or his/her child posts on social media, for example, could be used by others, including private companies and law enforcement in some cases, and is not protected by POPIA.

7.8.2 Parents and learners must understand and use the privacy tools on any website or app that the school provides (or what they use for school or at home) to limit who can view or access their information - that includes having strong, secure and unique passwords and be sure to never post anything online that they wouldn't want shared with others, including law enforcement, the school, tertiary institutions, and current or future employers.

7.9 Consent to Process Personal Information

7.9.1 In terms of POPIA, a "Responsible Party" (in this case being the school) has a legal duty to process a "data subject's" personal Information (in this case being the personal information and related details of a parent/legal/guardian/care giver and/or any enrolled learner and/or any employee of the school and the WCED and/or any other person) in a lawful, legitimate, and responsible manner. (Annexure D)

7.9.2 In order to discharge this duty, the school requires the express and informed permission to process the Personal Information of a data subject or any other third party.

7.9.3 In the event of any data subject or third party or any other person, refusing to give the required consent, the school will still have the right, in terms of POPIA, to process such information without the mentioned consent under any of the following circumstances:

a. where such processing and use of personal information is necessary in order to give effect to a contractual relationship as between the person and the school.
b. where such processing is required in terms of a law, such as without limiting the generality thereof:
    i. the Basic Conditions of Employment Act 75 of 1997(BCEA),
    ii. the Labour Relations Act
    iii. the Skills Development Act, 97 of 1998(SDA),
    iv. Skills Development Levies Act, 9 of 1999 (SDLA)
    v. the Employment Equity Act, 55 of 1998
    vi. The Employment of Educators Act
    vii. The Unemployment Insurance Contributions Act, 4 of 2002 (UICA) Unemployment Insurance Act, 6 of 2001 (UIF),
    viii. Financial Advisory And Intermediary Services Act, 37 of 2002 (FAIS), the Financial Intelligence Centre Act 38 of 2001 (FICA),
    ix. the National Credit Act, 34 of 2005 (NCA)
    x. the Compensation for Occupational Injuries and Diseases Act, 130 of 1993,
    xi. Children's Act
    xii. The Disaster Management Act and all related regulations with regard to COVID-19;
    xiii. The Occupational Health and Safety Act
    xiv. National Education Policy Act, 1996 (Act No. 27 of 1996), as amended
    xv. Criminal Law (Sexual Offences and Related Matters) Amendment Act (Act no 32 of 2007)
    xvi. 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")
    xvii. Regulations for Misconduct of Learners at Public Schools and Disciplinary Proceedings, 2001 (General Notice 2591 of 2001).
    xviii. Drugs and Drugs Trafficking Act (Act 140 of 1992)
    xix. Child Justice Act 75 of 2008.
    xx. Medicines and Related Substances Act No 101 of 1965, As Amended.

xxi. Regulations for Safety Measures at Public Schools Government Notice No. 1040, October 2001, as amended.
xxii. Guidelines for the Consideration of Governing Bodies in Adopting a Code of Conduct for Learners, General Notice 776 of 1998.
xxiii. Regulations to Prohibit Initiation Practices in Schools, GN No. 1589, 13 December 2002
xxiv. the Schools Act, Act 84 of 1996, as amended and any related regulations and/or provincial legislation and/or related regulations and/or policies and policies of the school.

c. Where such processing is necessary to protect the legitimate interests of the school or a third party.

7.10 Privacy Policy and Privacy Notice

7.10.1 A Privacy Policy prescribes and defines the handling practices and obligations that staff must abide by when processing personal information.

7.10.2 A Privacy Notice sets the tone and defines the school's data privacy mission statement for the school's external stakeholders and data subjects.

7.11 Specific Purpose Collection of Information

7.11.1 Personal Information must be collected for a specific, explicitly defined and lawful purpose by the school related to the function or activity of the responsible party. The data subject must be made aware of the purpose of the collection.

7.12 The POPIA Act's Eight Conditions for Lawful Processing of Information Adhered to by the School

7.12.1 POPIA issues its rules for using South African data in Chapter 3 of the Act. It refers to these rules as conditions, and they largely cover what data may be collected, what can be done with the data, and how to protect both the data and the data subject.

7.12.2 POPIA includes eight conditions for lawful processing including:

a. Accountability.
b. Processing limitation.
c. Purpose specification.
d. Further processing limitation.
e. Information technology [quality].
f. Openness.
g. Security safeguards.
h. Data Subject participation.

7.12.3 A brief overview of each condition is as follows:

7.12.3.1 **Condition 1: Accountability**

It stipulates that the responsible party has the responsibility of ensuring the rest of the conditions are in place before processing data. The responsible party must also **ensure compliance** both when deciding to process data and during the processing of the data.

7.12.3.2 **Condition 2: Processing Limitation**

The Processing Limitation - places strict controls on what it means to lawfully process data. To meet the condition, data processors must:

a. Process data in a way that **does not risk** the data subject's privacy.
b. Process **only relevant data** with a given purpose.
c. **Obtain the consent** from the data subject before processing (and keep proof of consent).
d. Protect the **legitimate interest** of the data subject.
e. Allow Data Subjects to **object to processing and/or withdraw consent** at any time.
f. Discontinue with the processing of data after an objection or withdrawal of consent received for a data subject.
g. Condition 2 also provides a **unique** stipulation: "Personal information must be collected directly from the data subject" except for in specific circumstances. The only time the school can collect data from a third-party source is if the data is a public record or is deliberately made public or if the school has the consent to do so or if doing so does not violate the legitimate interest of the data subject. There are no exceptions for those working in the school with the processing of data.

7.12.3.3 **Condition 3: Purpose Specification**

Where Condition 2 limits the data the school can collect, Condition 3 the "Purpose Specification", details the reasons for collecting data.

a. The idea that the school must collect information only for a "specific, explicitly defined and lawful purpose" related to one of the school's normal activities is at the heart of POPIA.
b. Moreover, the school must ensure that data subjects are aware of that purpose.
c. The school may not retain records indefinitely. Once the school no longer needs a record for the processing purpose, it no longer has a right to keep the data unless required by law (civil, penal, contract, or other law).
d. The school must destroy, delete or de-identify the record as soon as practical.
e. The said process should render the data irretrievable.

7.12.3.4 **Condition 4: Further Processing Limitation**

1. Conditions 2 and 3 aren't the only processing limitations. Condition 4 the "Further Processing Limitation", continues to elaborate on how the school can and can't process data.
2. The main point to be noted is that the school must only process data in ways compatible with the purpose the data it is needed for.
3. In the case of condition 4 POPIA requires the school to consider the relationship between further processing and the original purpose, the nature of the information, potential consequences of further processing, how the school collected the data, and any contractual rights.
4. The school can always further process data if:
    a. The data subject consented.
    b. The information came from the public record.
    c. The law requires further processing.
    d. The processing is related to national security.

7.12.3.5 **Condition 5: Information Technology or Quality**

1. Condition 5 indicates that the school must take steps to ensure the data collected and subsequently processed is accurate and complete.

7.12.3.6 **Condition 6: Openness**

1. Openness refers to the school's responsibility under the Promotion of Access to Information Act (PAIA). Essentially, the school must maintain strict documentation of all the processing activities it undertakes. Additionally, the school has to inform data subjects when it collects information.

2. Data subjects should be aware:
    a. Under which circumstances, the school collects information.
    b. When the school does not collect information.
    c. The source of the school's information
    d. The school's address and contact details.
    e. Why the school collects the data (the school's purpose for collecting data).
    f. Whether the collection of data by the school from a data subject is voluntary or mandatory.
    g. What will happen if the data subjects do not provide their data to the school as requested.
    h. The relevant legislation that allows for data collection from data subjects.
    i. This must all be shared before the school collects information from the data subject.
    j. Condition 6 also requires the school to have a Privacy Policy.

7.12.3.7 **Condition 7: Security Safeguards**

1. Condition 7 details the security measures POPIA requires for personal information. In the Act it is indicated that the school must employ "appropriate, reasonable, technical and organisational measures" designed to prevent both unlawful access and the loss or damage of the personal information. The school shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:
    a. Identify all reasonably foreseeable risks to information security; and
    b. establish and maintain appropriate safeguards against such risks. To meet these obligations, the school must perform a risk assessment test, ensure the maintenance of safeguards, verify the effectiveness of the safeguards, and ensure new updates are provided to prevent new deficiencies or risks.
2. POPIA also indicates that anyone processing personal information must also only first gain the knowledge of authorisation of the school and consider the information to be confidential. Any other (third) parties who process information on behalf of the school must sign a written contract and notify the school if there is a breach.
3. Condition 7 also provides a list of requirements if the school believes its security is compromised. First, the school must notify the Regulator and the data subject (when possible) and they must do so as soon as reasonably possible.
4. Data subjects must be notified in writing by email, letter, a news article, or by publishing an alert on a prominent part of the school's website. The Regulator may also direct the notification efforts as they see fit.
5. The notification must include enough information for the data subject so that they know what measures to take to protect themselves against further breaches.
6. Finally, the Regulator may require the school to publicise the breach if the Regulator believes doing so is reasonable.
7. Written records will be kept secure:
    a. Personal Information records should be kept in locked cabinets, or safes.
    b. When in use Personal Information records should not be left unattended in areas where non-staff members may access them.
    c. The school shall implement and maintain a "Clean Desk Policy" where all educators and staff shall be required to clear their desks of all personal information any kind when leaving their desks for any length of time and at the end of the day.
    d. Personal Information which is no longer required should be disposed of by shredding and a record kept
    e. Any loss or theft of, or unauthorised access to, personal information must be immediately reported to the Information Officer or the Deputy Information Officers
8. Electronic records of any kind will be kept secure:
    a. All electronically held Personal Information must be saved in a secure database.
    b. As far as reasonably practicable, no Personal Information of data subjects of the school should be saved on individual computers, laptops, or hand-held devices.
    c. All computers, laptops and hand-held devices should be access protected with a password, fingerprint, or any other access control method being of reasonable complexity, and changed frequently.

d. All staff of 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.
e. Electronic Personal Information which is no longer required must be deleted from the individual laptop, handheld device or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.

9. Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer and/or Deputy Information Officers, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.
10. Passwords and Access: Users have a responsibility to safeguard any credentials granted to them by the school. In order to limit security risks, all users must abide by the following:
    a. Attempts should not be made to by-pass or render ineffective security measures provided by the school.
    b. Users may not:
        i. Share user IDs or usernames.
        ii. Divulge passwords to other users.
        iii. Attempt to impersonate other users.
        iv. Leave their computer unattended without logging out or locking.
        v. Share passwords between users, except where they are released as part of the approved procedure. An approved procedure exists for releasing passwords where accounts are required, and staff are unavailable.

7.12.3.8 **Condition 8: Data Subject Participation**

1. Condition 8 describes the rights of a data subject. In terms of POPIA, the data subjects have access to their personal information, including taking note of what information the school has and the option to ask for a description or record.
2. The data subject also has the right to request corrections to his/her record when the data is out of date, incomplete, inaccurate, excessive, or obtained unlawfully.
3. Upon receiving the request, the school must adhere to the request within a reasonable timeframe.
4. The school has the option to decline when it falls within its rights as stated in Chapter 4 of the law.
5. Condition 8 also has several parts. Part B refers to the prohibition of processing of special personal information (including religious beliefs, health information, biometric information, etc.) or criminal behaviour.
6. The only exceptions that apply include:
    a. If the data subject provided consent.
    b. If processing is necessary for establishing a defence of a right.
    c. If processing is required for fulfilling obligations under international public law.
    d. If processing is in the public interest.
    e. If the data is already in the public domain.
    f. If processing involves historical research, or statistical purposes (within the public interest or if asking consent is impossible or close to impossible).
7. POPIA puts significant emphasis on these special categories of information and each type of data has a list of exemptions. If the school has to process a protected type of data, it should rather refer directly to the law and/or seek legal advice.

7.13 Data of Children

7.13.1 The school may not process children's personal information unless:
    a. The school has the consent of a "competent person" (parent/guardian/care giver/legal entity/authority).
    b. It is necessary for obligations under POPIA and other legislation.
    c. It is required for upholding international public law.
    d. It is necessary for research purposes.

7.13.2 The Regulator may also grant permission if it is in the public interest and the school agrees to use the appropriate safeguards. In addition, the Regulator may also impose further conditions related to the nature of the data, the amount of information, and the method of processing.

7.14 Processing of Information by using Automated and Non-automated Means

7.14.1 POPIA applies to the processing of any personal information by the school that has been entered into a record (by or for the school as the responsible party) by using automated and non-automated means.

7.14.2 This is subject to the proviso that when the recorded personal information is processed by any non-automated means, the record must from part of a filing system or is intended to form part of a filing system.

7.15 Performing a POPIA GAP Analysis and Risk Assessments

7.15.1 The school already takes care when processing data. However, the school has to identify what areas of POPIA compliance the school already meets and where the school is deficient. (Annexure C)

7.15.2 POPIA's security requirements require the Information Officer of the school to take necessary measures for protecting the school's information.

7.15.3 The GAP analysis is unique to the school. As a baseline, the school should know that the school's IT infrastructure and personnel resources should allow it to engage in best practices for data safety and security.

7.15.4 The GAP analysis and risk assessments should normally be started early in project development or design, or before a new data processing activity, and must be considered throughout the data's lifecycle from collection to destruction.

7.15.5 The risk assessment/GAP analysis is an opportunity to identify the school's security strengths, weaknesses, and to ensure that management can cope with the threats the school faces.

7.15.6 The risk assessment, is also an analysis of how personally identifiable information (PII) of data subjects are collected, used, shared, stored, filed and maintained by the school.

7.15.7 The GAP analysis can reveal where the school has weaknesses when it comes to protecting the personal data it collects, stores and uses.

7.15.8 Processes have to be put in place to collect data only for a specific purpose: to inform the Data Subjects of the reason for collection, and to have a process for safely deleting/destructing the data when it has served its purpose.

7.15.9 To sum it up, here are some questions to answer when the school is undertaking assessments:

a. Does the school have the appropriate legal authority to collect the personal data?
b. Have the school received consent from the data subjects to use their data?
c. Is the school using out-of-date or irrelevant personal data to make decisions?
d. Is the school disclosing data to third parties that it is not authorised or who do not keep personal data appropriately secure?
e. Does the school have processes in place to dispose of private data after use?

7.16 General Description of Information Security Measures

7.16.1 The school uses up to date technology/software to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

a. Firewalls.
b. Virus protection software and update protocols.
c. Logical and physical access control.
d. Secure setup of hardware and software making up the IT infrastructure.
e. Outsourced third party service providers are contracted to implement security controls on a regular basis.

7.17 Access and Security to Information/Records

7.17.1 Personal information shall be managed in terms of the school's Privacy Policy and POPIA

7.17.2 For health and safety reasons, the school reserves the right to check on the usage and content of any files, messages, pictures, images, or similar which are created, received, stored, transferred to, viewed, read, sent from or received using a cell phone or other device present on school property (whether or not it belongs to the school), at a school or school-sponsored function or activity, or on the way to school or school-sponsored activity, regardless of whether the device was actually used on school property, at a school function or not.

7.17.3 Records in all formats, shall always be protected against unauthorised access and tampering to protect their authenticity and reliability as evidence of the business of the school.

7.17.4 Security classified records shall be managed only by authorised persons.

7.17.5 No staff member shall remove records in any format that are not available in the public domain from the premises of the school without the explicit permission of the Information Officer in consultation with the Chairperson of the SGB.

7.17.6 No staff member shall provide information and records that are not in the public domain to the public without consulting the Information Officer. Specific guidelines regarding requests for information are contained in the Promotion of Access to Information Policy which is maintained by the Information Officer.

7.17.7 No staff member shall disclose personal information of any member of staff or any other data subject to any member of the public without consulting the Information Officer first.

7.17.8 An audit trail shall be logged of all attempts to alter/edit electronic records and their metadata.

7.17.9 Records storage areas shall always be protected against unauthorised access. The following shall apply:

a. Registry and other records storage areas shall be locked when not in use.

7.17.10 Access to server rooms and storage areas for electronic records, media, and CCTV shall be managed with key card access or strict key control.

7.17.11 The school's access to the safes and the walk in safe and key controls policy will be adhered to.

7.17.12 **Paper-based records**

a. No records shall be removed from paper-based files without the explicit permission of the records manager.
b. Records that were placed on files shall not be altered in any way.
c. No alterations of any kind shall be made to records other than correspondence files without the explicit permission of the records manager.
d. Should evidence be obtained of tampering with records, the staff member involved shall be subject to disciplinary action.

7.17.13 **Electronic records**

a. The school shall use systems which ensure that its electronic records are:
    i. authentic;
    ii. not altered or tampered with;
    iii. legible;
    iv. auditable; and
    v. produced/processed in systems which utilise security measures to ensure their integrity.

7.18 Signing of any document and the Purpose of a Signature on a Document

7.18.1 When a data subject who is entitled to do so signs a document the school assumes the following:

a. That the data subject has read the document in order to fully understand what he/she is signing and agreeing to.
b. That if anything is unclear, he/she has the right to ask for clarification and/or may obtain legal advice before signing.
c. Ensure that all blank spaces in the document are completed or scratched out and signed next to it.
d. If there is anything that has to be changed in the document, to make sure that the changes are made before signing the document.
e. Once the data subject has signed a document, he/she is legally bound by its contents.
f. For certain documents, an electronic signature will not be considered as a valid signature where it must still be in a physical form and signed by hand.
g. If a person cannot sign a document himself/herself (either owing to being illiterate or owing to a physical condition that prevents him/her from writing) he/she may sign the document with a mark (such as an 'X') or using a thumbprint. It might be necessary to make the mark or thumbprint in the presence of a commissioner of oaths or a notary.
h. It is also possible for a representative to sign a document on behalf of someone else or an entity such as the SGB or a company, however the representative must be authorised in writing or by a resolution or a power of attorney to do so.

7.19 Witnessing documents

7.19.1 The purpose of a witness is to verify the signature of a person who is a party to a contract or other document.

7.19.2 The witness is needed to confirm that the correct party has signed the document and no fraud has occurred, such as someone signing the document on another person's behalf.

7.19.3 In certain other matters, it is legally required to witness certain documents, like statutory declarations or affidavits in legal proceedings, to have the signature witnessed by a person with specific qualifications (an authorised witness).

7.19.4 There are also specific requirements for witnessing signatures on will documents such as powers of attorney.

7.19.5 A witness's signature can be useful for evidentiary purposes. If a party to the agreement later alleges, he/she did not sign, the person who witnessed the party signing can be called to confirm it. The witness can confirm that the specific person signed and that that was the signature they made.

7.20 Steps to Correctly Witness a Signature

7.20.1 When witnessing a signature, the witness must:

a. ensure that the person signs the document in front of the witness. It is not acceptable for him/her to provide the witness with a document that someone else has already signed and to request the witness, to witness it;
b. use black ink, as this will scan more clearly on electronic versions of the document;
c. check the person has signed where required on all pages of the document;
d. initial any changes that the person makes after signing the document;
e. check what additional details is needed to provide when witnessing, as set out on the document and provide them correctly. This may include the date, occupation and address of the witness; and
f. it must be possible for the witness to be traced at a later stage.

7.21 Certified Copies

7.21.1 Certified copies refer to a copy of a document that has been stamped by a Notary/Commissioner of Oaths to certify that the copy is a true copy of the original. And that is all it means. A certified copy does not verify the authenticity of the original document, only that the copy is a true copy of what appears to be an original document to the person certifying the copy.

7.21.2 Certified Copies can only be made of documents that are original. What makes something an original document is whether it has some sort of seal, stamp, or signature. Some types of documents that are very common to certify as true copies include such things as Identification Documents (e.g. Passport, Driver's License, Birth Certificate), Diplomas, Report Cards, etc.

7.21.3 The reason the school requires certified copies is to ensure that the original documents or ID books/cards and other forms of identification and FICA documents are genuine. This is to avoid fraud, where any person can make up certificates and documents on a computer that looks real. A certified copy also avoids the owner of important documents (especially identity documents) giving up possession of those documents which might mean a risk of their loss or damage.

7.21.4 To request certification of a copy of a document the Data Subject have to take both the original document and the copy to an authorised official which includes an official of SAPS, attorneys, some ministers of religion and/or the Principal of the School.

7.21.5 The following must be complied with when submitting certified copies as a copy of a true original document to the school:

a. Each document copy must be certified separately.
b. The certification date stamp must not be older than 3 months.
c. The full names and surnames, date, designation and signature of the Commissioner of Oaths who certify the documents.
d. The Commissioner of Oaths must write down or stamp that he/she certifies that the document is a true copy of the original document and that there is no indication that the original document has been altered in any way by an unauthorised person or persons.
e. The Commissioner of Oaths must append a signature and also print out his/her name, designation, contact particulars and date.

7.21.6 The person certifying a document should not be related to the person submitting the document, living at the same address as the person submitting the document or be in a relationship with the person submitting the document.

7.21.7 Failure to comply with the above with regard to certified copies will result in a document being rejected.

7.22 Common Acts of POPIA Non-Compliance:

7.22.1 Common examples of POPIA non-compliance are the following:

a. Loss or theft of paperwork/data/misfiling/not saving data.
b. Data posted or e-mailed or sent to incorrect recipient including on any groups on any social media App/platform.
c. Insecure webpage (including hacking).
d. Loss or theft of unencrypted device.
e. No or inadequate firewalls and/or anti-virus software.
f. Insecure disposal of paperwork.
g. Failure to redact data.
h. Sensitive or confidential Information uploaded to webpage.
i. Verbal disclosure without permission or carelessly done.
j. Insecure disposal of hardware.
k. Sending confidential data by e-mail/Apps that is not supposed to be circulated.
l. Sticky notes with PII data breach such as passwords or reminders.
m. Smartphone unsecured data breach.
n. Lost keys data breach/not keeping keys safe.
o. Lost digital/electronic items data breach (laptops, USBs, external hard drives etc.)
p. Easy access to computer room/offices.
q. Unlocked doors to empty classes/offices/walk in safe, server room.
r. Leaving file cabinets, desk drawers and cupboards open or documents on desks unattended.
s. Unsecured access card.
t. Forgotten documents in the printer/copy machine.
u. Forgotten PII on the whiteboard.
v. Responding to phishing e-mails/clicking on unsecure links.

7.23 POPIA and Internet Usage and Connections

7.23.1 The School's Internet connections are intended for activities associated with:

a. The work and information of the school.
b. The exercise by users of their responsibilities and duties.
c. The professional/academic development of staff and learners.

7.23.2 Internet access and e-mail shall not, for example, be used for the following:

a. Personal gain or profit.
b. For anyone to represent him-herself as somebody else
c. To advertise or otherwise support or engage in illegal activities.
d. To endorse any product or sponsor except if approved by the SGB.
e. To provide lists or information about the school or the school's staff, parents/ guardians/caregivers/agents/contractors, SGB members or learners to others and/or to send other confidential information without approval.

7.24 POPIA and E-mail Usage

7.24.1 Where needed, staff and learners (henceforth referred to as "users") within the school are provided with a school email account to assist with their work/duties for the school.

7.24.2 Email account holders must always comply with this Policy.

7.24.3 The email account of a user, and any information contained in it including content, headers, directories, and email system logs, remains the property of the school.

7.24.4 Users are responsible for the integrity of their mailbox. IT Services cannot restore any emails deleted accidentally or otherwise. All email messages may be subject POPIA and other legislation and laws of South Africa and any employment prescripts as amended, updated or replaced from time to time.

7.24.5 Although the school has systems in place to protect the integrity and safety of the school's electronic network, it must be noted that the school cannot guarantee the confidentiality of information stored on any network device belonging to the school.

7.24.6 Great care should be taken when attaching documents to ensure the correct information is being released.

7.24.7 Any email should be regarded as a written formal letter and data.

7.24.8 Any defamatory or careless remarks can have profoundly serious consequences. The use of indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise, is strictly prohibited.

7.24.9 Users are not authorised to retrieve or read any e-mail messages that are not sent to them or not for their attention, except when authorised under the approved procedure.

7.24.10 Email messages must not be automatically forwarded (redirected) to external non-school accounts such as a staff member's own personal e-mail account. Should a staff member or learner receive any offensive, unpleasant, harassing or intimidating messages via e-mail, he/she are requested to inform the Deputy Principal or Grade Head Co-ordinator immediately.

7.25 POPIA and Bulk Email

7.25.1 From time to time the school authorities may wish to communicate with parents via bulk email.

7.25.2 Such bulk e-mail lists must comply with the following:

a. Staff and members of the SGB may not send emails to the list which are obscene, abusive, or threatening.
b. The contents of emails must be courteous and show tolerance towards other users of the list.
c. Senders must be mindful of the fact that any messages will be widely published.

7.25.3 Therefore, users are expected to exercise restraint when voicing controversial opinions. In particular, they must:

a. Respect the variety of cultures and beliefs that are likely to be represented across such a large audience.
b. Ensure that any messages they send cannot be construed as being in any way defamatory.
c. Ensure that they do not damage the reputation of the school or any of its staff members/parents/learners/agents/contractors or undermine its overall mission.
d. Take care not to forward emails that were intended only to the sender's address, to the bulk distribution list.
e. Chain letters/emails of any sort should not be sent.
f. There must be no third-party commercial advertising using the school bulk email lists, unless authorised in advance by principal.
g. E-mail messages originating elsewhere in a private capacity must not be forwarded to the lists without the permission of the original sender.
h. Only material in keeping with the purpose of the lists should be sent and, in particular, should not include messages for which other dedicated services are provided.
i. Some lists are for official staff announcements only. These lists will be used for formal communication from designated school members of the SMT/EXCO. Permission to send to these lists will be restricted and authorisation will be granted by the principal/deputy principal. Replies to this type of message must not be sent to the whole list.

7.25.4 E-mail messages must be kept as short as possible and must contain only text:

a. Images, logos, 'watermark' backgrounds, etc. are to be used sparingly since they greatly increase the size of a message.
b. In general, messages should be sent only once. Exceptionally, official reminders and security/safety related messages may be repeated.

7.25.5 In the event of an IT Security issue the school reserves the right to stop bulk email lists until the threat has been mitigated.

7.26 POPIA and Personal Websites

7.26.1 The School recognises that from time-to-time staff will setup websites, blogs or wikis that, while related to their academic or professional disciplines, are personal sites and not formal school sites.

7.26.2 In this regard the purpose of the POPIA policy is to strike the appropriate balance of providing staff with the academic freedom to engage in open discourse, while also protecting the reputation of the school and that of its Staff and other members of the school community. In addition, these POPIA policy rules ensure that the individual views and opinions discussed openly on such sites are not portrayed as the formal position of the school at any time or under any circumstances.

7.26.3 Personal websites should not display the school crest, regalia, logo or other school trademarked/copyrighted materials, including the school designs, or otherwise appear to be an "official" school web page, unless with the permission of the Principal and the SGB.

7.26.4 The use of personal websites for the following purposes is strictly prohibited:

a. Any use which may have the effect of violating any laws (or exposing the school to unacceptable legal risk).
b. Any use which may adversely impact on school computing or on network resources.
c. Any use which the school considers may be defamatory or libellous.
d. Any use which may infringe the rights of any third party in respect of personal data, intellectual property or other confidential or proprietary information.
e. Making accessible materials which could have the effect of damaging the reputation and goodwill of the school.
f. Are otherwise in breach of this Policy.

7.26.5 On personal websites, staff members are required to identify views expressed as their own and that the staff member do not hold him-/herself out as representing the school. If an employee of the school identify him-/herself as being a member of Staff of the school, he/she must state clearly that any views expressed are not necessarily those of the school.

7.27 POPIA and Social Media

7.27.1 Social media is a collective term for websites and applications which focus on communication, community-based input, interaction, content-sharing and collaboration. Examples of social media include Facebook, WhatsApp, Twitter, Instagram, Snapchat, TikTok, Telegram, Signal, 9GAG, Reddit, and more.

7.27.2 The sharing and/or posting of Personal Information on social media is strictly prohibited unless consent has been obtained from the relevant data subject(s) and does not default on any aspect of this Policy.

7.27.3 Any posts made publicly in the private capacity of learner, parent, or staff member on social media sites such as Facebook, Instagram, Twitter, and more is not protected by the POPIA.

7.27.4 Any defamatory or careless remarks can have profoundly serious consequences. The use of indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise, is strictly prohibited.

7.27.5 The use of social media (whether it is in the data subject's personal- or work-related capacity) is subject to the provisions stipulated in the school's Code of Conduct and ICT Policy.

7.28 School Photographs/Images/Videos of Learners

7.28.1 Photographs, other images and sound recordings are often taken of learners, in many cases by professional photographers and at the school's request. Any photograph of one or more identifiable individual(s) is considered to be personal information.

7.28.2 The school is permitted to collect personal information, including photographs, where it is necessary to do the proper administration of a lawfully authorised activity, but the photographs/ images may not be released to a third party unless a parent's consent was obtained. The collection of learner photographs is considered necessary to the operation of the school (a lawfully authorised activity because, for example, photographs are used for ID cards, access cards and/or to enable staff to identify learners, provided the records are kept confidential).

7.28.3 If the school uses a professional photographer, the SGB/principal/Information officer is still ultimately responsible for the security and confidentiality of the learners' personal information/image.

7.28.4 Any service agreements with third party vendors must align with the provisions of POPIA.

7.28.5 Their contracts should clearly describe the administrative, physical and technical safeguards to protect personal information and the obligation to destroy any images if not handed over to the school for safekeeping.

7.28.6 The permission of parents may be obtained for the use of photographs for other purposes such as annual photos for parents, social media, the school website, printed media, or promotional purposes, provided that children at risk is not shown or their images pixelated.

7.28.7 Images and any other videos of learners on the school's website/social media must be disabled so that it cannot be copied or downloadable as far as possible.

7.29 SGB Employees' Information

7.29.1 Each appointed employee of the SGB will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part of the contract 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.

7.29.2 Each SGB employee currently employed within the school will sign an addendum to their Employment Contract or an undertaking 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 if not included. Failure to comply will result in the instigation of a disciplinary procedure.

7.29.3 Staff will sign relevant consent and confidentiality agreements/undertakings for purposes of processing their information in terms of POPIA processing.

7.30 CCTV

7.30.1 The school will post notices at every entrance gate and the entrance to the administration office informing persons on the school property that the school uses CCTV to monitor the school grounds. In order to:

a. protect and ensure personal safety of data subjects when on the school premises; and
b. to investigate, detect or prevent crime and to apprehend or prosecute offenders.
c. to monitor and record activities that are in plain view on the school's premises.

7.30.2 Data subjects must note that all audio or visual recordings that the school record/produce using CCTV cameras are records of the school**.**

7.30.3 The school must retain these records in accordance with the school's record retention schedules and policies.

7.31 Entry to the School Grounds by Parents and Visitors

7.31.1 The School and SGB reserve the right to:

a. Inspect any person and/or his/her property when entering the school premises.
b. Require each person to enter their details into a register and their ID may be checked to verify it is the person entering the premises.
c. The school may also record any details of a vehicle entering the premises.
d. The school may refuse any person entry to the school's premises at the Principal's discretion.

7.32 Bots

7.32.1 Bots are automated programmes that run over the Internet. Bots may be used responsibly by the school to facilitate the receipt of e-mails and other messages on social media platforms to acknowledge receipt of e-mails and other electronic information received, or to facilitate answering FAQs about the school on its website and other social media platforms.

7.33 Direct Marketing by Means of Unsolicited Electronic Communications

7.33.1 In terms of this Manual/Policy, direct marketing is the use of personal information for the purposes of direct marketing by means of any form of electronic communication or other forms of communication.

7.33.2 Direct marketing is ***PROHIBITED*** unless – the school has consent, or the data subject is already a parent of the school who has provided consent or a prospective parent who wants to enrol his/her child as a learner of the school, or a person who requests information with regard to the school that does not include any information of another person or data subject.

7.33.3 The school may only approach a person/data subject for consent, ***ONCE***, and if they have not previously withheld such consent. The school may only ***USE*** the information for the purpose it was obtained.

7.33.4 Any communication for the purpose of direct marketing from the school must contain:

a. Details of the identity of the sender of the school, or on behalf of the school clearly stated with the contact details of the person of the school who the receiver can make contact if they do not wish to deal with the sender; and
b. The address or other contact details to which the recipient may send a request to opt-out.

7.33.5 Obviously it is not possible to fit all information on some forms of communication (like an SMS/WhatsApp). In that case, the school can provide a link (in the form of a tiny URL like "T's and Cs") to a webpage that sets out the information.

7.34 Scanned documents

7.34.1 If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to any staff of the school.

7.34.2 Any document containing information of the written particulars of an employee, including the employee's name and occupation, time worked by each employee, remuneration and the date of birth of an employee under the age of 18 years the information must be retained for a period of 3 years after termination of employment.

7.35 Encryption of Personal Information

7.35.1 Encryption is a key technical measure for securing school data and the first line of defence. All electronic information must be encrypted where possible and passwords to access/decrypt personal information must be used.

7.36 Consolidating information using "THE CLOUD" to comply with POPIA

7.36.1 Should many copies of personal information exist in many different places it is exposed to a greater number of risks and breach. If the school can consolidate personal information into one encrypted safe central location in the cloud and then control the security and access to the data subjects' personal information, the school will be protecting personal information.

7.37 Data Portability

7.37.1 Data Portability is about moving or copying personal data from one place to another, whether it be from one data controller to another, or one IT system to another.

7.37.2 Section 20 of POPIA sets out the right that the data subject has to data portability. This means that the information that the data subject has provided to the data controller of the school must be able to be moved in a structured and commonly used format and to achieve this action the personal data must be portable.

7.38 Operating Controls

7.38.1 The SGB, the Principal, and SMT/EXCO of the school shall establish appropriate privacy standard operating controls that are consistent with this policy and regulatory requirements. This will include:

a. Allocation of information security responsibilities.
b. Incident reporting and management.
c. User ID addition or removal.
d. Information security training and education.
e. Data backup and retention of records.

7.39 Monitoring and Implementation of the Policy

7.39.1 The SGB, the SMT/EXCO, the Principal, if not the Information Officer and all operators, as defined by POPIA, are responsible for administering and overseeing the implementation of this policy manual and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes.

7.39.2 Periodic reviews and audits will be conducted by the Information Officer/Deputy Information Officers where appropriate, to demonstrate compliance with POPIA, any policies and guidelines.

7.40 Duty to Report a [Vulnerable] Child in Need of Protection

7.40.1 In terms of the Children's Act, any person, including professionals who work with children, must immediately report to the Principal, the CPU of SAPS and/or Social Services any concerns regarding any child that is or may be suspected at risk if they have reasonable grounds to suspect that a child needs protection and complete a Form 22.

7.41 Notifying Parents of Harm to Learners

7.41.1 The WCED requires school employees to report to the Principal if they become aware that a learner may have engaged in an activity that could result in their suspension or expulsion. If the Principal believes that a learner has been harmed as a result of this activity, he/she has a duty to notify the District Director/Circuit Manager, the SGB, and that learner's parent or guardian, and the parent or guardian of any other learner who engaged in the activity. However, there are limits on the nature and extent of personal information that can be shared.

7.42 Occupational Health and Safety

7.42.1 In terms of the Occupational Health and Safety Act, the SGB and /or the Principal or his/her delegate *a*nd other employers must advise an employee of any danger to their health or safety that they are aware of.

7.43 Retention of Personal Information Records

7.43.1 The school may retain Personal Information records as required by the Archives Act, POPIA, other acts and legislation unless a data subject objects thereto. If the data subject objects to the period of retention of his/her PII the school shall retain the records to the extent that it is needed or required by law for a shorter period.

7.44 Destruction of Documents

7.44.1 Documents may be destroyed by shredding it after the termination of the retention period specified herein, or as determined by the school from time to time.

7.44.2 Each department 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 for a further one year and if not requested destroyed.

7.44.3 The documents may be made available for collection by an approved document disposal company or destroyed by the school. All documents destroyed must be logged in the register.

7.44.4 Deletion of any electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered and logged in the register.

7.45 Records that cannot be found or do not exist or believed not to exist

7.45.1 When 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.

7.46 Personal Information No Longer Personal Information

7.46.1 De-identified personal information is not personal information. Personal information of a deceased person is not personal information, as it does not relate to a living natural person.

7.47 POPIA Complaints Procedure

7.47.1 Complaints may be filled via email to the school at info@settlers.org.za

7.48 Disciplinary Action

7.48.1 Where a POPIA complaint or a POPIA infringement investigation has been finalised, the school may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee or learner reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

7.48.2 In the case of ignorance or minor negligence, the school will undertake to provide further awareness training to the employee or learner.

7.48.3 Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the school may summarily dismiss the employee or recommend a learner for expulsion.

7.48.4 Disciplinary procedures will commence where there is sufficient evidence to support an employee's/learner's gross negligence.

8. AMENDMENTS

8.1 Modifications and updates to this policy manual and other information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

9. APPROVAL

Recommended by Principal: _____ **Signature:** _____ **Date:** _____
Approved by SGB Chairperson: _____ **Signature:** _____ **Date:** _____
Verification by WCED _____ **Signature:** _____ **Date:** _____
Certified by _____ **Signature:** _____ **Date:** _____

SCHOOL STAMP

10. ANNEXURES

ANNEXURE A: PERSONAL INFORMATION AND RECORDS HELD BY THE SCHOOL OF THE FOLLOWING DATA SUBJECTS

1. LEARNERS (AS DEFINED BY THE SOUTH AFRICAN SCHOOLS ACT NO 84 OF 1996)

a. Learner's application for admission to a public school indicating the following personal information:
   i. Name and Surname of the learner.
   ii. ID number of the learners.
   iii. Date of Birth.
   iv. A personal identifier such as a learner's EMIS and/or where applicable a LSEN number allocated by the WCED and/or account Number.
   v. Gender.
   vi. Race.
   vii. Physical address and contact details.
   viii. Medical and health information and where necessary medical report from medical doctor/physician/specialist/psychologist.
   ix. If applicable, records regarding a learner's primary disability.
   x. Home Language.
   xi. Learner's Cell number.
   xii. Learner's email address.

b. Certified copies of supporting documents as follows:
   i. Birth certificate;
   ii. ID documents;
   iii. Inoculation certificate;
   iv. Report cards from previous school;
   v. Study and asylum permits;
   vi. If applicable change of name/surname certificate and new ID details.

c. Learner profiles and documents in profiles.
d. Transfer Card (where applicable from previous school).
e. Disciplinary hearing records.
f. Debit record/Merit Record.
g. Promotion and assessment records.
h. Extra and Co-curricular records.
i. Behavioural records.
j. Photographs of learners/Copy of School access card.
k. Biometrics of learners.
l. CCTV footage of learners.
m. Documentation with additional information, such as custody orders or special education records.
n. Consent forms from parents for learners to attend field trips/tours/participation in sport or cultural activities.
o. Videos and voice recordings where applicable for processes such as disciplinary hearings or for use in psych-social support.
p. State-administered assessment results, including participation information, courses taken and completed, credits earned, academic grades, and other transcript information.
q. Grade level/Year and anticipated year of matriculating or completing schooling.
r. Attendance record and transfer information between and within school districts/provinces.
s. Special education data/assessments.
t. Schooling programme participation information required by the WCED/DBE or other government agencies.
u. Matric Examination numbers and registration records.

2. PARENTS (AS DEFINED BY THE SOUTH AFRICAN SCHOOLS ACT NO 84 OF 1996)

a. Certified copies of ID documents of parents.
b. Personal Information of parents:
    i. Full Name(s) and Surname.
    ii. Date(s) of birth and ID number(s)
    iii. Gender.
    iv. Race.
    v. Marital status.
    vi. Medical Aid.
    vii. Home and work physical and postal address
    viii. Landline and mobile telephone numbers.
    ix. Home and work email address (es).
    x. Profession and Employment details
    xi. Names of all the children in the family.
    xii. Home Language.
c. Financial record of school fee account:
    i. Ledger account.
    ii. Statement of account.
    iii. Receipts.
    iv. Journal entries.
    v. Correspondence and documents.
d. Application for exemption of school fees with the following supporting documents:
    i. Application form.
    ii. Proof of Income.
    iii. Bank Statements.
    iv. Other Financial documents proving income of parent.
    v. Documentation proving other children in the family.
    vi. Affidavits as needed.
    vii. Certified copies of court order letter from welfare agency/home if child is in care.
e. Compensation of school fees.
f. Correspondence with parents.
g. CCTV footage of parents.

3. EMPLOYEES EMPLOYED BY THE SCHOOL/SGB

a. Personal information of all employees
    i. Certified copies of ID documents.
    ii. Certified Copies of Diplomas/Degrees.
    iii. Personal contact details/e-mails/cell phone numbers.
    iv. Qualification certificates and certificates of workshops and training courses attended.
    v. Banking details.
    vi. Registration with statutory bodies SARS, UIF, Skills development, Workman's compensation.
    vii. Registration with SACE.
    viii. Curriculum Vitae.
    ix. References.
    x. Job Description.
    xi. Performance appraisals.
    xii. Contract of employment.
    xiii. Attendance registers.
    xiv. Medical records/Medical Aid/Biometric Information.
    xv. Leave application forms.
    xvi. Payroll administration records.
    xvii. Correspondence and letters of delegation.
    xviii. Disciplinary hearings records and written warnings.
    xix. Biometrics of employees.
    xx. Police clearance certificate.

xxi. Certified copiers of Driver's license – Professional Driving permits.
xxii. Photographs and copy of access card.
xxiii. Police Clearance Certificate.
xxiv. Pay slip registers.
xxv. Leave application forms.
xxvi. Claims expenses from School.

b. Personal Information of prospective employees:
   i. Interview scores.
   ii. CV and supporting documents.
c. Personal information past employees:
d. Documents as listed above in (a) not held on file longer than necessary.

4. EMPLOYEES EMPLOYED BY THE STATE

a. Personal information of all employees:
   i. Certified copies of ID documents.
   ii. PERSAL number.
   iii. Personal contact details/e-mails/cell phone numbers.
   iv. Certified Copies of Qualification certificates/Degrees.
   v. Salary scales.
   vi. Banking details.
   vii. Registration with SACE.
   viii. Curriculum Vitae.
   ix. References.
   x. Performance appraisals/IQMS.
   xi. Attendance registers.
   xii. Medical records/Medical Aid and Biometric information.
   xiii. Leave application forms.
   xiv. Letters of Delegation.
   xv. Pay slips issued by District.
   xvi. Pay roll administration record.
   xvii. Correspondence.
   xviii. Disciplinary hearings
   xix. Police Clearance Certificate.
   xx. Copy of Access Card.
b. Personal Information of prospective employees:
   i. Interview scores
   ii. CV and supporting documents.
   iii. SGB recommendations.
c. Personal information past employees
   i. Documents as listed above in (a).
d. Section 38 A SASA payments and claims expenses from School.

5. LEARNERSHIPS/STUDENTS/ASSISTANT EDUCATORS

a. Personal information of all learnerships/students/assistant educators
b. Certified Copies of ID documents.
c. Temporary SACE Registration.
d. Contact details/e-mails/cell phone numbers.
e. Contract agreement.
f. Performance appraisals.
g. Banking details.
h. Pay slips.
i. Pay slip register.
j. Correspondence.
k. Registration with statutory bodies SARS, UIF, Skills development, Workman's compensation.

l. Police Clearance Certificate.
m. Leave Application Forms.
n. Copy of Access Card.
o. Claims expenses from School.

6. TEMPORARY STAFF – COACHES, EDUCATORS, INVIGILATORS, ADMINISTRATORS, STUDENTS, ASSISTANT EDUCATORS

a. Personal information.
b. Certified Copies of ID documents.
c. CV and references.
d. Contact details/ e-mails/cell phone numbers.
e. Contract agreement.
f. Banking details.
g. Payroll records – Payslips.
h. Correspondence.
i. Police Clearance Certificate.
j. Claims expenses from School.

7. SUPPLIERS/AGENTS/CONTRACTORS AND OTHER PERSONS ("SUPPLIERS")

a. Personal information of all suppliers.
b. Financial records of all suppliers' account.
c. Contract agreements with all suppliers.
d. Correspondence with all suppliers.
e. Tender documents.
f. E-mails and Cell phone and landline numbers of individual representatives of suppliers.
g. Rental agreements such as office equipment.
h. Non-disclosure agreements.
i. Letters of intent (where applicable).
j. Outsourcing agreements (where applicable).

8. THE SETTLERS HIGH SCHOOL GOVERNING BODY AND SGB COMMITTEES

a. Personal information of all SGB members.
b. Contact details/e-mails/cell phone numbers and land line numbers.
c. Constitution of the SGB.
d. Budgetary Information.
e. Annual report to Parents' Budget meeting, minutes, attendance records and agendas.
f. Code of conduct of SGB.
g. Correspondence – general and specific.
h. Minutes of all meetings.
i. Agendas of Meetings.
j. Attendance Registers.
k. School Policies and Guidelines.
l. Copy of Access Card for School Premises.
m. Strategic Planning documents.

9. TENANTS

a. Personal Information details.
b. Lease agreements.
c. Correspondence.
d. Contract agreements with tenants.
e. Cell phone numbers/Landlines.
f. Payment account details.

10. NATIONAL GOVERNMENT DEPARTMENTS, THE DEPARTMENT OF BASIC EDUCATION AND THE WESTERN CAPE DEPARTMENT OF EDUCATION

a. Legislation - Acts, Regulations.
b. Circulars and Memos.
c. Guidelines.
d. Standard Operating Procedures.
e. Policies.
f. Curriculum assessment documents.
g. Minutes of District and Circuit meetings, agendas and presentations.
h. Whole school evaluation records.
i. Post establishment records.
j. Norms and Standards Allocation records.
k. Compensation for school fee exemption records.
l. Snap survey records.
m. Annual/ Quarterly/Monthly/weekly returns of statistics and data and audited financial reports.
n. Section 38A applications.
o. Approval application to open an Investment account.
p. Approval to obtain loan, extend, lease etc.
q. Correspondence hard copy and electronic messages.

11. PAST LEARNERS/ALUMNI

a. Personal Information details.
b. Contact details.
c. Correspondence/newsletters/invitations to school functions.
d. "Ed Labs" and personal profiles not requested by new school or after leaving school.
e. Copies of Transfer Cards.
f. Matric certificates/last record of attendance/report cards.

12. SPONSORS/DONORS/SUPPORTERS

a. Personal Information details.
b. Contact details.
c. Receipts – 18A.
d. Donation Register.
e. Correspondence.

13. ADVERTISERS

a. Personal Information details.
b. Invoices of payments.
c. Contact details.
d. Details of adverts.
e. Correspondence.

14. SPORTING BODIES/AFFILITIONS/CULTURAL BODIES

a. Personal Information details.
b. Contact details.
c. Subscriptions.
d. Correspondence.
e. Sporting Codes and rules.
f. Agendas and Minutes.
g. Financial Transactions/receipts.

15. ACADEMIC AUTHORITIES/ ASSOCIATIONS - SAQA, UMALUSI, SACE, IEB

a. Personal Information details.
b. Contact details.
c. Subscriptions.
d. Correspondence.
e. Registration lists of names and numbers.

16. SGB ASSOCIATIONS - FEDSAS, GBF

a. Personal Information details.
b. Contact details.
c. Newsletters.
d. Subscriptions.
e. Correspondence.

17. UNIONS - NAPTOSA, SAOU, PSA, SADTU AND OTHERS

a. Personal Information details.
b. Contact details.
c. Subscriptions.
d. Correspondence.
e. Case records.

18. STATUTORY BODIES - SARS – DEPARTMENT OF LABOUR- SETAS

a. Personal Information details.
b. Contact details.
c. Statutory returns.
d. Payment records.
e. Correspondence.
f. IRP 5s and other documents.

19. SCHOOL AUDITORS

a. Personal Information details.
b. Letter of appointment from the SGB.
c. Contact details.
d. Certificates of their registration with an authorising body/bodies/SAIPA.
e. Signed off Audit reports.
f. Contract of service.
g. Statement of account.
h. Financial statements.
i. Correspondence.
j. Internal Auditors records and reports.

20. INSURANCE HOUSES

a. Personal Information details.
b. Contact details of Representative/Broker.
c. Insurance agreement(s)/contracts.
d. Claim form.
e. Proof of payments.
f. Proof of claims paid out.
g. Correspondence

21. BANKING INSTITUTIONS

a. Personal Information details.
b. Correspondence who has signing authority/EFT authority.
c. Contact details of Banking Representative.
d. Record of accounts kept at the institution.
e. Correspondence.
f. Monthly banking transactions records/statements.
g. Cheque books.
h. Cancelled Cheques.
i. Print outs from computer re payments and transactions.
j. Debit card machine records and transaction slips.
k. Banking fees records.

22. ATTORNEYS / DEBT COLLECTORS /LEGAL COUNSEL

a. Personal Information details.
b. Contact details.
c. Records of case referred to them.
d. Contract entered into with 3rd party.
e. Their account and payments.
f. Correspondence and records.
g. Other documents.

23. OUTSOURCED PAYROLL (Where Applicable)

a. Personal information details of company.
b. Contact details.
c. Contract with company.
d. Financial records – pay slips.
e. Monthly accounts and payments.
f. Correspondence.

24. OUTSOURCED CLEANING SERVICES AND OTHER SERVICES (Where Applicable)

a. Personal information details of company.
b. Contact details.
c. Contract with company.
d. Statement of account and payments.
e. Invoices and Delivery Slips.
f. Correspondence.

25. OUTSOURCED IT/OFFICE EQUIPMENT (Where Applicable)

a. Personal information details of company.
b. Contact details.
c. Statement of account and payments.
d. Contract with company.
e. Delivery slips of supplies, software and equipment.
f. Statement of account.
g. Service visits.
h. Correspondence.

26. TRUSTEES/OLD BOYS ORGANISATION/OLD GIRLS ORGANISTION/SCHOOL SUPPORTERS' CLUBS/PARENTS'ORGANISATION

(Where Trusts/ organisations/ Committees/Clubs who have no direct impact on the School donates funds, goods, services etc. at arm's length)

a. Personal information details of each trustee/member.
b. Names of Executive Committee and details/Trustees.
c. Certified copies of ID documents of each trustee.
d. Trust documents and Copy of Deed of Trust.
e. Record of donations etc.
f. Minutes of meetings.
g. Correspondence.
h. Constitution where applicable.
i. Registration as Non-Profit Organisation where applicable.

27. EDUCATIONAL INSTITUTIONS (UNIVERSITIES/OTHER TERTIARY INSTITUTIONS) (Where Applicable)

a. Information of institution and representative/Registrar's Office.
b. Contact details.
c. Correspondence.

28. INFORMATION TECHNOLOGY

a. IT policies and procedures
b. Network diagrammes.
c. User Manuals.
d. Software licences.
e. Antivirus/Malware software.

29. SCHOOL RECORDS

a. Constitution.
b. Strategic Plan – Development Plan and Improvement Plan and Whole School Development.
c. Class lists of learners.
d. Grade Educator and Subject Educators Lists.
e. School Policies
    i. Admission Policy
    ii. Financial Policy
    iii. Language policy
    iv. Assessment policy
    v. LTSM policy
    vi. Religion policy
    vii. Anti-Bullying policy
    viii. HR policy
    ix. Tour policy
    x. Extra curricula policy and Sport Policy.
    xi. Hostel policy (Where Applicable)
    xii. Pregnancy policy
    xiii. Health and Safety policy
    xiv. Drug use policy
    xv. Homework policy
    xvi. Attendance and absentee policy
    xvii. Social Media policy
    xviii. School Transport policy

xix. Learner Code of conduct policy
xx. Other related policies and legislation.

f. Financial records
   i. Financial Ledgers and books of first entry.
   ii. Budgets.
   iii. Financial statements.
   iv. Annual Audited Financial Reports.
   v. Reports on Financial matters.
   vi. Bank statements and records.
   vii. Invoices and receipts.
   viii. Details of all investment accounts.
   ix. Payroll records.
   x. List of all assets and inventory.
g. Incident Records.
h. Curriculum documentation.
i. Learner Assessment records.
j. Lease agreements.
k. Contracts.
l. Agendas, attendance records and Minutes of meetings.
m. LTSM records.
n. School Magazines/Newsletters/Annuals.
o. Timetable records/Rosters.
p. Asset Registers.
q. Procurement and Acquisition records.
r. Organogramme of school.
s. IT policies and procedures.
t. CCTV recordings and sound recordings.
u. Software programmes:
   i. Pastel
   ii. Payroll software (VIP, Pastel).
   iii. Administrative software (Pencil Box, Edusolutions, Principal Primary, SASPAC, SASAMS etc.).
   iv. Microsoft Office Suite.
   v. Library programmes (LIBWIN) (Where applicable).
   vi. Backups of all records and disaster recovery.
   vii. Antivirus and Malware Programmes, Firewalls.
   viii. Biometric/Card entrance points scanning programmes.
   ix. User manuals.
   x. Network security controls.
   xi. Passwords controls.
v. Internal forms.
w. Correspondence.
x. Class lists/attendance rosters.
y. Duty Rosters.
z. Records of marks for tests and assignments.
aa. Photographs of learners with their names.
bb. Honour rolls of learners.
cc. Other types of progressive discipline records such as debit and positive discipline records.
dd. Motor vehicle records.

ANNEXURE B: FUNCTIONS OF THE INFORMATION OFFICER, DEPUTY INFORMATION OFFICERS, AND INFORMATION OPERATORS

1. Introduction

Section 32 of the Constitution guarantees every person the right of access to information. Every individual, including juristic persons or natural persons, has the right to access information held by the state or any other person in order to assist him or her to exercise or protect his or her rights. It is required that the school have to appoint an Information Officer and/or Deputy Information Officers in terms of the Protection of Personal Information Act (POPIA) 4 of 2013 and the Promotion of Access to Information Act (PAIA) 2 of 2000.

2. Who is the Information Officer or who should be appointed as one?

In terms of Section 1 of PAIA, the Information Officer will include the following persons:

(a) in the case of a national department, provincial administration or School al component-

(i) mentioned in Column 1 of Schedule 1 or 3 to the Public Service Act, 1994 (Proclamation No. 103 of 1994), means the officer who is the incumbent of the post bearing the designation mentioned in Schedule 1 or 3 opposite the name of the relevant national department, provincial administration or School component or the person who is acting as such; or

(ii) not so mentioned, means the Director-General, head, executive director or equivalent officer, respectively, of that national department, provincial administration or School component, respectively, or the person who is acting as such…

The Principal will accordingly fulfil the role of Information Officer for the school and he or she is at liberty to appoint Deputy Information Officers from the School's corps of educators and/or the Deputy Principal(s).

3. Responsibilities of an Information Officer

The responsibilities of the Information Officer include, but are not limited to, the following:

a. To compile a manual setting out the structure and functioning of operations of the public body. This manual must be made available in three (3) official languages.
b. The information officer of a public body may delete any part of a record which, on a request for access, may or must be refused.
c. The information officer of a public body has direction and control over every deputy information officer of that body
d. The information officer of a public body may delegate a power or duty conferred or imposed on that information officer by this Act to a deputy information officer of that public body. The delegation should be in writing and can be revoked at any stage.
e. An individual who because of illiteracy or a disability is unable to make a request for access to a record of a public body, may make that request orally. The information officer of that body must reduce that oral request to writing and provide a copy thereof to the requester.
f. The information officer should provide reasonable assistance free of charge to those requesting information.
g. The information officer may not refuse requests if such requests are not made in the prescribed form, unless the information officer notified the requester of his or her intention to refuse the request, provided reasons for the refusal and provided assistance to the requester to make the request in the prescribed manner.
h. The information officer must provide a requester with a reasonable opportunity to request assistance, must provide the requester with any information that would assist the requester in making a request and provide the requester a reasonable period to confirm or amend a request in order to comply with the prescribed format.
i. The information officer has to ensure that, in the event that a request is directed at the wrong public body, the request is referred to the correct public body or information officer within 14 days.
j. The information officer has to ensure that the prescribed fees are paid (if applicable) before a request is processed.

k. In the event that records cannot be traced or found, the information officer should testify through a sworn affidavit that all reasonable steps have been taken to trace the documents or to confirm that the documents do not exist. The affidavits should also contain the correspondence between the persons involved in the search conducted on behalf of the information officer.

4. Duties of an Information Officer (delegated to Deputy Information Officers)

The duties of the Information Officer are prescribed by POPIA itself, as well as the regulations. The duties include, but are not limited to, the following:

a. To ensure compliance with both POPI and PAIA
b. To ensure the school is registered with the Information Regulator
c. To deal with requests for access to personal information
d. To cooperate with the regulator in the event of investigations initiated against the school
e. To ensure that compliance frameworks are developed, implemented, monitored, and maintained
f. To ensure that a personal information impact assessment is conducted and to ensure that sufficient measures and standards exist in order to comply with the requirements regarding the legal processing of personal information
g. To ensure that a manual is developed, monitored, maintained, and made available
h. To ensure that internal measures are developed, in conjunction with complete systems to deal and process any requests regarding access to information
i. To ensure that internal awareness programs pertaining to the Act as well as the regulations to the Act are conducted, and to ensure that a code of conduct, or information from the Regulator can be obtained and kept.
j. If any copies of the manual are sought, such copies should be provided to the person subject to payment of a fee as determined by the Regulator.

5. Information Operators

Under the guidance of the Information Officer (IO) and Deputy Information Officers (DIO), each department within the school will have an appointed Information Operator (IOP).

Who the Information Operators are for a particular department will depend on the yearly review of management portfolios by the Principal. In general, all Departmental Heads (Post Level 2) and Deputy Principals (Post Level 3) are to be considered Information Operators.

The duties of an Information Operator include, but are not limited to, the following:

a. To assist the IO and DIO to ensure compliance with both POPI and PAIA
b. To assist the IO and DIO with requests for access to personal information
c. To assist the IO and DIO in the event of investigations initiated against the school
d. To assist the IO and DIO in performing a personal information impact assessment and/or risk assessment for their respective department.
e. To ensure that sufficient measures and standards are implemented within their respective department to comply with the requirements regarding the legal processing of personal information
f. To ensure that internal measures for their department are developed, in conjunction with complete systems to deal and process any requests regarding access to information

ANNEXURE C: DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

1. Background

Section 19 of the Protection of Personal Information Act POPIA determines that:

> *(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent — (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information;*
>
> *(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to — (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; (b) establish and maintain appropriate safeguards against the risks identified; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards;*
>
> *(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.*

The **"responsible party"** means the governing body of the school which determines the purpose of and means for processing personal information.

In order to comply with this section and POPIA, the steps a responsible party must take for appropriate, reasonable technical and organisational measures include:

- **Identify risks** – identify all risks to the personal information;
- **Create safeguards** – create safeguards for those risks;
- **Check safeguards** – check that those safeguards are working;
- **Update safeguards** – and update those safeguards for any new risks.

The measures that the school must take, have to address:

- The existing and prospective risks to the personal information in the school's possession or under its control;
- The most recent level of development of technology at a particular time; and
- The costs of creating, checking, and updating safeguards for those risks in terms of money, time, and labour.

2. Data Protection Impact Assessment

2.1 A Data Protection Impact Assessment (DPIA) is a process to assist the school in identifying and minimising the data protection risks of the school.

2.2 A DPIA is a way for the school to systematically and comprehensively analyse data processing and assist the school to identify and minimise data protection risks. It is an important tool for building and demonstrating compliance with POPIA (i.e. accountability).

2.3 In terms of POPIA the School must carry out a DPIA/GAP analysis where a planned or existing processing operation is "*likely to result in a high risk*" to individuals. Although POPIA and its regulations provide examples of data processing that would fall into this category, this is a non- exhaustive list.

2.4 It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

3. Purpose

3.1 The purpose of this procedure is to enable School Staff to:

a. identify when a DPIA is mandatory;
b. carry out a DPIA.

4. Scope

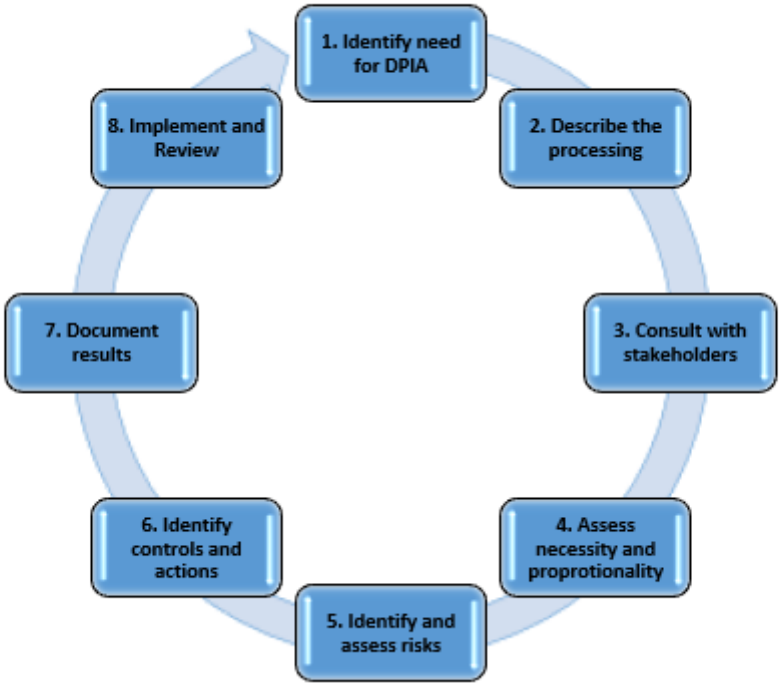
4.1 All administrative and data collection and significant changes to existing systems/processes which require the processing of personal data must perform at least step 1 of this procedure to determine if a full DPIA is required.

4.2 DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of data subjects, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non- material.

4.3 To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on all data subjects, information collection, storing of records and staff and other persons.

4.4 A DPIA does not have to eradicate the risks altogether but should help to minimise risks and assess whether or not remaining risks are justified.

5. Proposed DPIA Procedure



<u>Step 1: Identify the Need for a DPIA/whether a DPIA is mandatory</u>

POPIA does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of persons. The school must do a DPIA if the school plans to carry out one or more of the following:

1. **Evaluation and scoring (including profiling and predicting)**, especially concerning a Data Subject's performance at work, economic situation, health, personal preferences, reliability or behaviour, location or movements. An example would be offering genetic tests in order to assess or predict disease/health risks or gathering social media profile data for generating profiles for contact directories or marketing.

2. **Automated decision-making with legal or similar significant effects -** is a decision made by automated means without any human involvement? An example would be an online decision to award a loan or a recruitment aptitude test that uses pre-programmed algorithms and criteria.

3. **Systematic monitoring** - including through a publicly accessible place on a large scale. For example, using CCTV and academic results or employee performance.

4. **Special data or data of highly personal nature** – this includes special categories of data as defined:
    a. racial or ethnic origin;
    b. political opinions;
    c. religious or philosophical beliefs;
    d. trade union membership;
    e. data concerning health;
    f. data concerning a person's sex life or sexual orientation;
    g. genetic data;
    h. biometric data;
    i. as well as criminal data.

5. **Data processed on a large scale** – while the term 'large scale' is not defined, the following should be taken into account:
    a. the number of data subjects concerned;
    b. the volume and range of data been processed;
    c. the duration and permanence of the processing;
    d. the geographic extent of the processing activity;
    e. keeping records and data.

6. **Datasets have been matched or combined** – for example, two or more data processing operations performed for different purposes and/or by different data controllers been combined in way that would exceed reasonable expectation of the data subject.

7. **Data concerning vulnerable data subjects** – for example children are considered as not able to knowingly oppose or consent to processing of personal data and considered vulnerable data subjects.

8. **Innovative use or applying technological or organisational solutions** – for example combining use of fingerprint and access cards for improved physical access control.

9. **When processing prevents the Data Subject from exercising a right or using a service or a contract** – for example, processing in a public area that people passing cannot avoid or processing that aims to refuse data subjects access to a service (exemption of school fees) or participating in a school activity.

10. In cases where it is not clear if a DPIA should be carried out, then a DPIA ***should*** be carried out as it is a useful tool to comply with POPIA.

<u>Step 2: Describe the Processing in a Systematic Way</u>

Describe how and why the school plan to use the personal data. The school's description must include "*the nature, scope, context and purposes of the processing*".

1. The nature of the processing
   This is what the school plans to do with the personal data. This must include:
    a. how you collect the data;
    b. how you store the data;
    c. how you use the data;
    d. who has access to the data;
    e. who you share the data with;
    f. whether you use any processors;
    g. retention periods;
    h. security measures;
    i. whether you are using any new technologies;

j. whether you are using any novel types of processing;
k. which data screening criteria you flagged as likely high risk.

2. **The scope of the processing**
   This is what the processing covers. This must include:
   a. the nature of the personal data;
   b. the volume and variety of the personal data;
   c. the sensitivity of the personal data;
   d. the extent and frequency of the processing;
   e. the duration of the processing;
   f. the number of data subjects involved;
   g. the geographical area covered.

3. **The context of the** processing
   This is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:
   a. the source of the data;
   b. the nature of your relationship with the persons;
   c. the extent to which persons have control over their data;
   d. the extent to which persons are likely to expect the processing;
   e. whether they include children or other vulnerable persons;
   f. any previous experience of this type of processing;
   g. any relevant advances in technology or security;
   h. any current issues of public concern;
   i. whether the school has considered and complied with relevant codes of practice.

4. The **purpose of the processing**
   This is the reason why the school wants to process the personal data. This must include:
   a. the school's legitimate interests, where relevant;
   b. the intended outcome for data subjects providing information;
   c. the expected benefits/legal obligations for the school.

Step 3: Assess Necessity and Proportionality

One should consider:
1. Do your plans help to achieve your purpose?
2. Is there any other reasonable way to achieve the same result?
3. your lawful basis for the processing;
4. how you will prevent function creep i.e. using the data for more than the original purpose;
5. how you intend to ensure data quality;
6. how you intend to ensure data minimisation;
7. how you intend to provide privacy information to individuals;
8. how you implement and support individual's rights;
9. measures to ensure your processors comply;
10. safeguards for international transfers.

Step 4: Consult with Stakeholders

You should seek the views of data subjects (or their representatives) unless there is a good reason not to. In most cases it should be possible to consult individuals in some form. For example, internal stakeholders such as project management team, IT, procurement, potential suppliers (processors), communications teams, customer facing roles, researchers and senior management. External stakeholders could include: people who will be affected by the project and members of the public.

However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of your DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing students or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views. If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.
If you use a data processor, you may need to ask them for information and assistance. You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security.

Step 5: Identify and Assess Risks

Identify the potential risks that may arise. Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

1. inability to exercise rights (including but not limited to privacy rights);
2. inability to access services or opportunities;
3. loss of control over the use of personal data;
4. prevent discrimination;
5. identity theft or fraud;
6. financial loss;
7. reputational damage;
8. physical harm;
9. loss of confidentiality;
10. re-identification of pseudonymised data;
11. any other significant economic or social disadvantage.

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). Having identified the risks, it is then necessary to assess which are going to pose the greatest threat by looking at both the likelihood of the risk occurring and the impact that might result. This provides the overall risk rating.

Step 6: Identify Controls and Actions

Against each risk identified, you should then consider options for reducing that risk. Identify the current controls (how you currently manage the risk) and what further actions you will take to reduce the impact/likelihood and mitigate the risk. For example, some actions and controls that could be implemented are:

1. deciding not to collect certain types of data;
2. reducing the scope of the processing;
3. reducing retention periods;
4. taking additional technological security measures;
5. training staff to ensure risks are anticipated and managed;
6. anonymising or pseudonymising data where possible or as needed;
7. writing internal guidance or processes to avoid risks;
8. adding a human element to review automated decisions;
9. using a different technology;
10. putting clear data sharing agreements into place;
11. making changes to privacy notices;
12. offering individuals the chance to opt out where appropriate;
13. implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks. You should ask the Information Compliance Office for advice.

Step 7: Document Results

You should then record:

1. what additional measures you plan to take;
2. whether each risk has been eliminated, reduced, or accepted;
3. the overall level of 'residual risk' after taking additional measures;
4. whether the Data Protection Commission needs to be consulted.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to contact the Information Compliance Manager who will consult with the Data Commissioner before you can go ahead with the processing. As part of the sign-off process, you should ask the Information Compliance Manager to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons. You should also record any reasons for going against the views of individuals or other consultees.

Step 8: Implement and Review

You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them. You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised. If you have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, you need to consult the Data Commissioner before you can go ahead with the processing.

It is good practice to publish your DPIA to aid transparency and accountability. This could help foster trust in your processing activities and improve individuals' ability to exercise their rights. If you are concerned that publication might reveal commercially sensitive information, undermine security or cause other risks, you should consider whether you can redact (black out) or remove sensitive details, or publish a summary. You need to keep your DPIA under review, at a minimum every 3 years. You may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

ANNEXURE D: RISK ASSESSMENT/INFORMATION SECURITY CHECKLIST

1. Purpose

1.1 The Risk Assessment/Information Security Checklist is a tool to aid the school in determining its current status with regards to POPIA and PAIA compliancy.

1.2 The tool must be completed and/or updated whenever this policy is reviewed to ensure continued awareness, implementation, and compliancy from all concerned parties.

2. Information Operators

2.1 The following Information Operators (IOP) are responsible for the completion of the risk assessment/information security checklist for their department:

DEPARTMENT	INFORMATION OPERATOR (as at last review of this policy)
Administration	Mrs Gallie
Academic/Assessment/Curriculum Administration	Mrs Gallie, Mrs de Kock, Ms Dyck, Mr Sass
Amenities	Mrs Gallie, Mr Vergotine
Ceremonies & Admin Publications	Mrs Heinz
Communications	Mr Nieuwoudt
Contact	Mrs Adams
Counselling	Ms Frieslaar
Culture	Mr Sass
Finance/Fundraising	Mrs Gallie, Mrs van der Berg, Mr Damonse
Human Resources	Mrs Gallie, Mrs Diederiks, Mr Damonse
IT	Mrs B Kleinsmith
Library/Print Room	Mrs Davids
Operations	Mrs Minnie
Safety & Security	Mrs Peacock
Sport	Mrs Basheer
Pastoral	Mrs Magson

3. Risk Assessment/Information Security Checklist

3.1 This risk assessment/Information Security Checklist is not exhaustive and may be adapted at the review of this policy.

3.2 The tabular structure allows for easy completion with the following key:

KEY	DESCRIPTION OF KEY
✓	Measure in place
✗	Measure not in place
H	High Impact / High Priority
M	Medium Impact / Medium Priority
L	Low Impact / Low Priority

ADMINISTRATION DEPARTMENT				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Admission Forms: Do we obtain permission from parents to collect and process information?	✓		
2	Are learner profiles (including birth certificates, ID's, parent information, contact details etc.) kept in a secure space with only authorised access?	✓		
3	Do we have a process in place for when educators need a learner's profile?	✓		
4	Do we have a process we can follow when another school requires information pertaining to our current and past learners?	✓		
5	Do we have a process of how we securely send transfer cards to other schools?	✓		
6	Is there someone who controls teacher absenteeism and doctor's notes?	✓		
7	Are minutes of SGB meetings encrypted/password protected before being emailed or distributed?	✗	**H**	**H**
8	Are the minutes of SGB meetings kept in a secure location with only authorised access?	✓		
9	Are the minutes of SMT meetings kept in a secure location with only authorised access?	✓		
10	Are all hard-copy documents containing personal information removed from desks when a staff member is not present and/or the door locked to prevent access to these documents?	✓		

ACADEMIC/ASSESSMENT/CURRICULUM ADMINISTRATION				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are electronic academic and assessment records kept in a secure location and password-protected or encrypted?	✓		
2	Are minutes/reports/notes of a SAIC securely stored?	✓		
3	Are report cards sent electronically to parents password protected and/or encrypted?	✗	**H**	**H**
4	Are report cards sent physically to parents sealed in an envelope?	✓		
5	A lot of the school's data is transferred to the Education Department via CEMIS or just physically. Have we obtained assurance from the Education Department that his information is secure?	✗	**H**	**H**
6	Are there measures in place to restrict staff access to learner data in the electronic school management system to only what is required as part of their job?	✗	**M**	**M**

AMENITIES				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are employee records kept securely and only accessible to authorised staff?	✓		
2	Have employees signed the necessary consent forms?	✗	**H**	**H**

CEREMONIES & ADMIN PUBLICATIONS				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are invitations sent directly to the person without the address or personal information from other possible attendees visible.	✓		
2	Have staff been informed that learner results for verification and awards are confidential?	✓		
3	Will information for guests be kept secure?	✓		
4	Have all staff (teaching and non-teaching) been informed that their staff manual must be kept secure as it contains personal information of others?	✓		
5	Have suppliers and service providers signed the POPIA agreement?	✓		

COMMUNICATIONS				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Have all parents/learners completed the educational marketing consent form?	✗	**H**	**H**
2	Is there a procedure in place for learners whose parents object to them been photographed?	✗	**H**	**H**
3	Do educators forward intellectual property of the school to other school/colleagues? Do they obtain permission to do so?	✗	**H**	**H**
4	Are there measures to ensure sensitive or confidential information uploaded to webpage, social media sites etc. are above board?	✓		
5	Are all electronic communication methods (including email, SMS, WhatsApp, Telephone etc.) encrypted and securely transmitted?	✓		
6	Are records/recordings from electronic communication securely stored and or encrypted?	✓		
7	Have measures been put in place to ensure that communication is sent directly to recipient without compromising the personal/confidential information of other recipients?	✓		
8	Are all hard-copy documents containing personal information removed from desks when a staff member is not present and/or the door locked to prevent access to these documents?	✗	**H**	**H**
9	Are sensitive documents containing personal information shredded or otherwise securely disposed of?	✓		
10	Have the school's website been locked to prevent images or videos downloaded without permission?	✗	**H**	**H**

CONTACT				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are new staff members trained on the importance of POPIA?	✖	**H**	**H**
2	Have all new staff members signed the consent form for the school to use their personal information?	✖	**H**	**H**

COUNSELLING				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are the clinical notes stored securely?	✖	**H**	**H**
2	Are clinical notes disposed of safely?	✖	**H**	**H**
3	Are the lever-arch files stored securely?	✖	**M**	**M**
4	Is the appointment notebook/register stored securely?	✖	**H**	**H**
5	Is the room locked and secured when unattended?	✖	**H**	**H**
6	Are emails sent to/received from parents and learners kept secure?	✓	**-**	**-**

CULTURE				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are the details of visitors to cultural events kept in a secure location?	✓		
2	Is the information of learners participating in cultural activities/societies kept confidential and secure?	✓		
3	Have all learners participating in cultural activities signed the consent form?	✖	**H**	**H**

FINANCE/FUNDRAISING				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
	General:			
1	Are there measures in place to make regular, secure, backups of electronic as well as physical financial records?	✓		
2	Are the annual financial statements kept in a secure location with access granted to only authorised staff?	✓		
3	Are financial reports presented to SGB kept in a secure location with suitable measures in place to protect the information?	✓		
4	Are all hard-copy documents containing personal information removed from desks when a staff member is not present and/or the door locked to prevent access to these documents?	✓		
5	Are sensitive documents containing personal information shredded or otherwise securely disposed of?	✓		
6	Are our auditors cleared for access to our school's financial records and do we have a privacy agreement with them?	✓		
	Debtors:			
7	Are statements sent to parents encrypted and/or password protected?	✓		
8	Is the Financial Assistance Form for exemption from school fees POPI compliant?	✓		
9	Are current Financial Assistance Forms for exemption from school fees with supporting documents securely stored?	✓		
10	Are separate statements and/or forms sent for divorced parents?	✓		
11	Is there a written agreement from debt collectors or attorneys that parent data will be kept safe?	✓		
12	When Financial Assistance for exemption of school fees list is presented at FINCOM are parents' name omitted?	✓		
	Creditors:			
13	Do we have the POPI Service Provider Agreements signed and stored from all our service providers?	✓		
14	Do we have the necessary measures in place to ensure only authorised staff are allowed to load and release payments?	✓		
	Payroll:			
15	Is the payroll system secure and prevents unauthorised access?	✓		
16	Are salary slips password-protected and/or encrypted when sent to staff?	✓		

HUMAN RESOURCES				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Has consent been obtained from employees to collect their personal data?	✗	**H**	**H**
2	Are employee files kept in locked cabinets and/or a secure space?	✓		
3	Employees who have retired or resigned, are their documents kept for 5 years thereafter?	✓		
4	Are CVs for prospective applicants destroyed if applicant is not successful?	✓		
5	Are employee grievances, warnings, and disciplinary hearing notifications securely stored?	✓		
6	Is the list of staff salary or the renumeration received by employees only accessible to authorised staff?	✓		
7	When staff leave, is there a handover form and do they sign that all intellectual property of the school has been deleted from their devices?	✓		
8	Are all hard-copy documents containing personal information removed from desks when a staff member is not present and/or the door locked to prevent access to these documents?	✓		
9	Are sensitive documents containing personal information shredded or otherwise securely disposed of?	✓		
10	Are the IQMS/QMS records securely stored with limited access?	✓		
11	Are the whole school evaluation records kept in a safe place?	✓		
12	Are staff and learners encouraged/made aware of the importance of security whether it be personal information or not?	✓		

IT DEPARTMENT				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Is there a back-up policy?*	✖	**L**	**L**
2	Is there an access control policy?	✓		
3	Is there an Internet usage policy?	✓		
4	Is there an email usage policy?	✓		
5	Is there a hardware security policy?	✓		
6	Is there a malware protection policy?	✖	**L**	**L**
7	Is there a removable storage media policy? *	✖	**L**	**L**
8	Is there a "clear screen" policy? *	✖	**L**	**L**
9	Is there a "Bring your own Device" policy? *	✓		
10	Are all computers password-protected? *	✖	**H**	**H**
11	Are passwords changed on a regular basis?	✖	**L**	**L**
12	Is two-factor authentication activated where possible?	✖	**L**	**L**
13	Are staff/learners expected to log off or lock their computers when leaving them unattended?	✓		
14	Are there procedures in place for dealing with breaches of security? *	✖	**L**	**L**
15	Are their measures in place to prevent unauthorised access to the network from users? (Firewall)	✓		
16	Are there procedures in place for dealing with, and definitions of, unacceptable use of computer equipment? *	✓		
17	Are there procedures in place to update malware/antivirus protection software regularly? *	✖		
18	Is there a plan to prevent/recover loss of service/contents/computer records?	✓		
19	Is the server room (and other critical equipment stored within) secured from unauthorised access?	✓	**L**	**L**
20	Is critical and/or sensitive data encrypted?	✓		
21	Are members of staff given laptops / tablets? Have they signed for the assets and usage there of? They load intellectual property, and they need to remove it when they leave.	✓		
22	Is there training for staff and learners on how to create/ensure a secure digital work environment?	✓		
23	Are there structures in place to prevent users from exporting data * without permission or to limit the ability to export data out of school?	✖	**L**	**L**
24	Are procedures to ensure that disposed electronics, storage devices, and other e-waste are scrubbed from any personal/confidential information?	✓		
25	Does the school do regular penetration testing – simulated attacks by a professional service provider on the school's computer system, network – to identify and address vulnerabilities?	✖	**L**	**L**
26	Are staff and learners made aware of the potential social engineering dangers and how to protect themselves from it?	✓		
27	Are public or multi-user computers secured in such a way as to prevent personal/confidential information from being accessed without authorisation? *	✖	**H**	**H**

**Note: The items are to be included in the new TSHS ICT Policy.*

LIBRARY/PRINT ROOM				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are sensitive documents printed securely stored until collected?	✓		
2	Is the learner information in the library secure?	✓		
3	Are obsolete files/documents shredded?	✓		

OPERATIONS				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Is sensitive data kept in a secure location?	✓		

SAFETY AND SECURITY				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are the COVID-19 screening data kept in a secure location?	✓		
2	Is there a plan in place to ensure that important records (hard copies as well as electronic) are protected from disaster or theft?	✓		
3	Do all doors have locks and can windows be securely closed to prevent unauthorised access?	✓		
4	Are all storage containers (cabinets, cupboards, safes etc.) and that contain sensitive information lockable and secure?	✓		
5	Are the recordings of the CCTV camera system accessible only to authorised staff members?	✓		
6	Are there CCTV cameras at key locations to prevent unauthorised access?	✓		
7	Is there a system in place to ensure that alarm codes are secure?	✓		
8	Are access cards/tags not currently in use removed from the system or blocked?	✓		
9	Is staff and learner biometric data for access control securely stored and encrypted?	✓		
10	Are security personnel cleared, identifiable, and do they patrol the school to prevent security breaches?	✓		
11	Are there procedures in place should a security breach occur?	✓		
12	Are there venues available to have safe, secure, and private discussions?	✓		
13	Have staff and learners been made aware of "tailgating" and the dangers surrounding it?	**x**	**M**	**M**

SPORT				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Are the personal information of external coaches securely stored?	✓		
2	Are disciplinary records stored securely?	✓		
3	Are the contact details for staff and coaches kept secure?	✓		
4	Are staff and other schools made aware of the confidential nature of inter-school documents.	✓		
5	Are sport-related insurance documents kept secure?	✓		
6	Are the minutes of the meetings kept secure?	✓		

PASTORAL				
	DESRIPTION OF RISK	**Measures/ Safeguards in Place?**	**Impact if not in Place?**	**Priority for Action Plan**
1	Learner Disciplinary Hearings: Are all the minutes and evidence kept in a secure location?	✓		
2	Learner Discipline Level 1 and 2 issues: Are records kept in a secure location?	✓		
3	Learner Detention Records: Are records kept in a secure location?	✓		
4	Grade Head Learner Information: Are these records stored in a secure location?	✓		
5	RCL/Prefect/Class Representative information and process of election: Is this information stored in a secure location?	✓		
6	House Committee Selection records: Are these kept in a secure location?	✓		
7	Staff Records and Discipline Issues: Are these minutes and records kept in a secure location?	✓		
8	Staff Information: is this information securely stored?	✓		
9	Parent Information of Staffroom: Is this information stored in a secure location?	✓		

ANNEXURE E: CONSENT FORMS IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)

1. **Consent Form for Parents/Learners**
2. **Consent Form for Staff**
3. **Consent Form to Receive Educational Marketing Material**

THE SETTLERS HIGH SCHOOL
CONSENT FORM TO USE PERSONAL INFORMATION OF PARENTS AND LEARNERS

I, the undersigned legal Parent/Guardian of _____ *(Child Name and Surname)* hereby authorise The Settlers High School to collect/store/process/use/share my personal information as well as the personal information of my child as stipulated in *The Settlers High School Policy Manual for The Protection of Personal Information and The Retention of Documents and Records in terms of the POPIA* (or "TSHS POPIA Policy") available on the school's website at https://www.settlers.org.za/

I therefore acknowledge that I have read the Policy in full and understand that:

1. The personal information the school collect/store may include information such as:
    - identity and contact details;
    - images/photos (including CCTV footage);
    - family details;
    - admission/enrolment details;
    - previous schools;
    - academic progress;
    - CEMIS number;
    - special educational needs;
    - nationality;
    - language;
    - religion;
    - medical information;
    - information about behaviour and attendance;
    - information about health, safety and welfare;
    - financial information (re fees, scholarships etc); and
    - other personal information.

2. The school uses/processes the personal information provided for the following purposes:
    - application for enrolment;
    - to provide appropriate education and support;
    - to monitor academic progress;
    - to care for our staff and learners;
    - to process applications, fees and scholarships;
    - to coordinate, evaluate, fund and organise educational programmes;
    - to comply with our legal obligations as an education body in terms of the Western Cape Provincial School Education Act, 1997;
    - to comply with our monitoring and reporting obligations to National and Provincial Government bodies in terms of the South African Schools Act, 1996;
    - to process appeals, resolve disputes, and defend litigation;
    - to send important circulars and information via email, SMS, or any other communication channels;
    - for social media, school website, newspaper publications, and school publications when appropriate; and
    - other necessary operations to fulfil our commitment as an educational institution.

3. The school shares personal information with third parties, including other National and Provincial Education bodies, and that the level of sharing and the nature of what is shared depend on various factors.

   The Government bodies to which the school transfers personal information will use the personal information for their own purposes (including: to verify other information they already hold about you, etc.) and they may aggregate it with other information they already hold.

   The school also shares personal information with other third parties, some of which include:
   - eiffelcorp (https://www.eiffelcorp.co.za/) – School Administration System
   - Google (https://www.google.co.za/) – Google Services such as Gmail & Google Classroom
   - d6 Group (https://d6.co.za/) – School Communicator
   - Karri (https://karripay.com/) – Cashless Payment System
   - Our Insurance Company
   - Our Legal Advisors

4. I have the following legal rights that can be exercised at any time:
   - Right to complain to the school.
     - Phone: 021 948-6116
     - Email: info@settlers.org.za
     - Postal Address: The Settlers High School, PO Box 599, Bellville, 7535
   - Right to complain to the Office of the Information Regulator.
     - Email: complaints.IR@justice.gov.za
     - Postal Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
   - Right of access to my or my child's personal information.
   - Right to rectification of any personal information that is not accurate.
   - Right to object to the processing of me or my child's personal information.

   Your complaint should include a brief description of what happened, when it happened and what personal information was affected.

5. The consent given is effective immediately and will remain effective until one of the conditions stated under Chapter 3, Section 14 of the Protection of Personal Information Act (POPIA), 2013 have been met.

_____	_____
Initials and Surname of Parent/Guardian	Full Name and Surname of Learner
_____	_____
Signature of Parent/Guardian	Date

THE SETTLERS HIGH SCHOOL
CONSENT FORM TO USE PERSONAL INFORMATION OF STAFF MEMBERS

I, the undersigned _____ *(Full Name and Surname)* hereby authorise The Settlers High School to collect/store/process/use/share my personal information as stipulated in *The Settlers High School Policy Manual for The Protection of Personal Information and The Retention of Documents and Records in terms of the POPIA* (or "TSHS POPIA Policy") available on the school's website at https://www.settlers.org.za/

I therefore acknowledge that I have read the Policy in full and understand that:

1. The personal information the school collect/store may include information such as:
    - identity and contact details;
    - images/photos (including CCTV footage);
    - family details;
    - nationality;
    - language;
    - religion;
    - medical information;
    - information about health, safety and welfare;
    - financial information; and
    - other personal information.

2. The school uses/processes my personal information provided for the following purposes:
    - to provide appropriate education and support;
    - to care for our staff and learners;
    - to process fees and payments;
    - to coordinate, evaluate, fund and organise educational programmes;
    - to comply with our legal obligations as an education body in terms of the Western Cape Provincial School Education Act, 1997;
    - to comply with our monitoring and reporting obligations to National and Provincial Government bodies in terms of the South African Schools Act, 1996;
    - to process appeals, resolve disputes, and defend litigation;
    - to send important circulars and information via email, SMS, or any other communication channels;
    - for social media, school website, newspaper publications, and school publications when appropriate;
    - to allow for communication between staff members (email, SMS, WhatsApp, Intercom); and
    - other necessary operations to fulfil our commitment as an educational institution.

4. The school shares personal information with third parties, including other National and Provincial Government bodies, and that the level of sharing and the nature of what is shared depend on various factors.

    The Government bodies to which the school transfers personal information will use the personal information for their own purposes (including: to verify other information they already hold about you, etc.) and they may aggregate it with other information they already hold.

The school also shares personal information with other third parties, some of which include:

- eiffelcorp (https://www.eiffelcorp.co.za/) – School Administration System
- Google (https://www.google.co.za/) – Google Services such as Gmail & Google Classroom
- d6 Group (https://d6.co.za/) – School Communicator
- Karri (https://karripay.com/) – Cashless Payment System
- Our Insurance Company
- Our Legal Advisors

4. I have the following legal rights that can be exercised at any time:
   - Right to complain to the school.
     - Phone: 021 948-6116
     - Email: info@settlers.org.za
     - Postal Address: The Settlers High School, PO Box 599, Bellville, 7535
   - Right to complain to the Office of the Information Regulator.
     - Email: complaints.IR@justice.gov.za
     - Postal Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
   - Right of access to my personal information.
   - Right to rectification of any personal information that is not accurate.
   - Right to object to the processing of my personal information.

   Your complaint should include a brief description of what happened, when it happened and what personal information was affected.

5. The consent given is effective immediately and will remain effective until one of the conditions stated under Chapter 3, Section 14 of the Protection of Personal Information Act (POPIA), 2013 have been met.

_____
Initials and Surname of Staff Member

_____ _____
Signature of Staff Member Date

THE SETTLERS HIGH SCHOOL
CONSENT FORM TO USE PERSONAL INFORMATION TO RECEIVE EDUCATIONAL MARKETING MATERIAL

Dear Parents

We often receive educational marketing material from third parties/affiliates which may be of use to you and your child. These include, but are not limited to:

- Tertiary Institution Information (Bursaries, Application Offers, Promotions, etc.)
- Workshops/Training Courses for Parents and Learners (Study Methods, Coping with Anxiety, etc.)
- Extra Tuition (Tenacious Tutors, Summer and Winter Revision Programmes, etc.)
- Free Educational Software/Online Resources
- and more.

In terms of the Protection of Personal Information Act (POPIA), we are not allowed to forward you any such material or information without your express permission.

We would therefore appreciate it if you would kindly complete the section below indicating to us whether you would like to receive educational marketing material or not.

I, the undersigned _____ *(Full Name and Surname),*

☐ hereby authorise The Settlers High School to use my personal information to send me educational marketing material in the form of SMS's, emails, d6 Communicator, and the like, subject to the following provisions:

1. My personal information is not shared with any third party for marketing purposes without my approval.
2. I have the right to withdraw my consent by notifying the school via email at info@settlers.org.za
3. The school is indemnified from any repercussions brought forth from me or my child using the educational material sent and/or services received.

☐ would prefer **not to receive any educational marketing material** at all. I understand that, in the case of the d6 Communicator, I will have to ensure that I am not subscribed to the relevant channel to avoid receiving educational marketing material. I also acknowledge that I cannot hold the school responsible for educational material/opportunities myself or my child miss out on as a result of this decision.

_____
Initials and Surname of Parent/Guardian

_____ _____
Signature of Parent/Guardian Date

ANNEXURE F: POPIA - SERVICE PROVIDER AGREEMENT TEMPLATE (FULL)

THE SETTLERS HIGH SCHOOL
PROTECTION OF PERSONAL INFORMATION
SERVICE PROVIDER AGREEMENT FORM

The parties to this agreement are

THE SETTLERS HIGH SCHOOL

(a public school and juristic person created in terms of section 15 of the South African Schools Act 84 of 1996 duly represented by the School Governing Body)

and

_____ (*name of service provider*)

(A natural person, full names and identity number; or a corporate entity, description and registration number)

WHEREBY IT IS AGREED THAT:

1. The service provider is hereby appointed by the school for the rendering of the services and/or supply of the goods as follows:

Description of goods and/or service to be supplied/is being supplied to the school:	
Fee to be paid/is being paid by the school to the service provider for the rendering of services and/or supply of the goods	
Effective Date *(yyyy/mm/dd)*	
Date of Completion *(yyyy/mm/dd)*	

This agreement may be renewed on an annual basis on the date of expiry of the initial term mentioned above, unless any of the parties informs the other to the contrary in writing at least one calendar month prior to the expiry date.

2. SERVICE LEVELS

2.1 The service provider undertakes to render the services in a proper, skilled, and competent manner, conforming to reasonable standards required by trade custom appropriate to the rendering of the services.

2.2 The service provider shall supply the goods in good order and condition, fit for the intended purpose.

2.3 Without derogating from the generality of the aforesaid, the service provider shall furthermore adhere to such service levels as may be agreed in writing between the parties from time to time.

3. FEES

3.1 The school shall pay the service provider the fees set out above and/or as described in the separate service agreement document that was signed, for the rendering of the services and/or supply of the goods.

3.2 The fees shall be payable on the dates agreed upon.

4. RIGHTS AND DUTIES OF THE SCHOOL

4.1 The school shall fully cooperate with the service provider to enable the latter to perform its duties in terms of this agreement.

4.2 The school or the agents of the school shall at all reasonable times be entitled to inspect the services rendered or goods supplied by the service provider to ensure that the terms of this agreement are adhered to and will be entitled to enter the service provider's business premises for this purpose.

5. CONFIDENTIALITY

5.1 The service provider shall at all times keep confidential the school's confidential information and shall not disclose any such information to any person, unless required in the normal course of the service provider's business or in the school's best interests.

5.2 The service provider may process the information provided only as authorised by the responsible party.

5.3 Upon the termination of this agreement, the service provider shall return to the school all records, papers, data, correspondence and other documents concerning and containing any reference to the school's business within seven days of receiving a written request to this effect.

6. PROTECTION OF PERSONAL INFORMATION

6.1 The service provider hereby undertakes to secure the integrity and confidentiality of all the information that the school discloses to the service provider and which the service provider has in its possession or under its control by introducing appropriate, reasonable technical and organisational measures. This will be done in accordance with the standards and prescripts set by the Protection of Personal Information Act (POPIA) 4 of 2013.

6.2 The service provider must notify the school immediately where there are reasonable grounds to believe that the school's information held by the service provider has been accessed or acquired by any unauthorised person.

7. INDEMNITY AND REPRESENTATION

7.1 The service provider hereby indemnifies the school, its employees and agents against all proceedings, damages, claims, costs and expenses incurred by reason of any claim in connection with the rendering of the services and/or supply of the goods.

7.2 The service provider shall not be entitled to incur any liability on behalf of the school, or in any way pledge or purport to pledge the school's credit.

8. CESSION AND ASSIGNMENT

The service provider shall not be entitled to cede its rights and assign its obligations hereunder without the school's prior written approval, which shall not be unreasonably withheld.

9. BREACH

9.1 Should any party to this agreement breach any term or condition thereof, the offended party shall give the offending party written notice to remedy such breach within fourteen days of receipt of the notice. Should the offending party fail to remedy such breach, the offended party shall be entitled to terminate this agreement with immediate effect.

9.2 This clause will not derogate from any common law rights that any of the parties may have against the other in the event of any breach of contract.

10. GENERAL

10.1 This agreement constitutes the entire agreement between the parties, and the parties will not be bound by any warranties or representations, whether express or implied, not stated herein.

10.2 No agreement at variance with the terms and conditions of this agreement, and no consensual cancellation of this agreement or any of its terms, will be binding on the parties, unless reduced to writing and signed by or on behalf of the parties.

10.3 No relaxation or indulgence granted by either party to the other will in any way prejudice or be deemed to waive either party's rights herein.

10.4 The school chooses domicilium citandi et executandi for all purposes under this agreement at:

_____

_____

_____

(insert physical address, postal address, fax number and e-mail address)

10.5 The service provider chooses domicilium citandi et executandi for all purposes under this agreement at:

_____

_____

_____

(insert physical address, postal address, fax number and e-mail address)

10.6 The parties agree to the jurisdiction of the magistrate's court, notwithstanding that the amount in issue may exceed the jurisdiction of such court.

THUS DONE AND SIGNED ON THIS ____ DAY OF _____ 20___.

AS WITNESSES:

1. _____ _____
SCHOOL
2. _____ (herein represented by the SGB)

THUS DONE AND SIGNED ON THIS ____ DAY OF _____ 20___.
AS WITNESSES:

1. _____ _____
SERVICE PROVIDER
2. _____ (herein represented by _____)

POPIA - SERVICE PROVIDER AGREEMENT TEMPLATE (ONLY POPIA)

THE SETTLERS HIGH SCHOOL
PROTECTION OF PERSONAL INFORMATION
SERVICE PROVIDER AGREEMENT FORM

The parties to this agreement are

THE SETTLERS HIGH SCHOOL

(a public school and juristic person created in terms of section 15 of the South African Schools Act 84 of 1996 duly represented by the School Governing Body)

and

_____ (*name of service provider*)

(A natural person, full names and identity number; or a corporate entity, description and registration number)

WHEREBY IT IS AGREED THAT:

1.1 The service provider hereby undertakes to secure the integrity and confidentiality of all the information that the school discloses to the service provider and which the service provider has in its possession or under its control by introducing appropriate, reasonable technical and organisational measures. This will be done in accordance with the standards and prescripts set by the Protection of Personal Information Act (POPIA) 4 of 2013.

1.2 The service provider must notify the school immediately where there are reasonable grounds to believe that the school's information held by the service provider has been accessed or acquired by any unauthorised person.

THUS DONE AND SIGNED ON THIS ____ DAY OF _____ 20___.

AS WITNESSES:

1. _____ _____
SCHOOL
2. _____ (herein represented by the SGB)

THUS DONE AND SIGNED ON THIS ____ DAY OF _____ 20___.

AS WITNESSES:

1. _____ _____
SERVICE PROVIDER
2. _____ (herein represented by _____)

ANNEXURE G: POPIA - RECORDS DISPOSAL REGISTER TEMPLATE

POPIA - RECORDS DISPOSAL REGISTER

DATE	RECORD TO BE DISPOSED	NAME OF EMPLOYEE REQUESTING RECORD TO BE DISPOSED OF	INFORMATION OFFICER APPROVAL FOR DISPOSAL	METHOD OF DISPOSAL

ANNEXURE H: POPIA – PERSONAL INFORMATION LOG TEMPLATE

PERSONAL INFORMATION LOG

This log is to be maintained by the Deputy IOs to reflect all objections received to the processing of personal information and a monthly report to be submitted to the IO and the SGB of the School for POPIA reporting purposes.

OBJECTION DATE	NAME OF PERSON WHO OBJECTED	PARENT OF LEARNER* (IF APPLICABLE)	DEPUTY IO SIGNATURE	COMMENTS