MCAULEY HOUSE SCHOOL

POLICY MANUAL FOR THE PROTECTION OF PERSONAL INFORMATION AND THE RETENTION OF DOCUMENTS AND RECORDS IN TERMS OF THE POPIA

Initialled by Chairperson of the SGB and the Principal _____

TABLE OF CONTENTS

Initialled by Chairperson of the SGB and the Principal _____

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

2. EFFECTIVE DATE: 01/06/2021

3. DATE OF NEXT REVIEW: 31/12/2021

4. REVISION HISTORY:

As amended on: 01/06/2021
Frequency of Review:
Annually or as needed

5. PREAMBLE

5.1. POPIA is not intended to prevent the processing of personal information but 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 processing of personal information must conform to the POPIA's provisions.

5.2. McAuley House School is a private 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 zero to twelve.

5.3. 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.

5.4. POPIA establishes the rights and duties that are designed to safeguard personal data in terms of POPIA, 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.

5.5. The school regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between the School and those persons also known as a data subject in terms of POPI 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.

5.6. Data (including information and knowledge) is essential to the administrative business of the school. In collecting personal data all staff has a responsibility to use it both effectively and ethically. There is a balance to be struck between an individual's right to privacy and the legitimate business requirements of the School. Therefore, it is critical that all staff in the Schoolwork 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.

5.7. Details of the School:

Postal address of the School: PO Box 91008
Auckland Park
2006

Street address of the School: Sans Souci Rd
Parktown West
2192

Telephone number of the School: 011 726 1310

E-mail address of the School: highschool@mcauleyhouse.co.za

The information officer is the principal, at date of inception of this policy Mr. Ross Davis, and he can be contacted in writing at: principalh@mcauleyhouse.co.za

The deputy information officer is principal of the primary school, Mrs Nichola Humphreys and she can be contacted in writing at principalp@mcauleyhouse.co.za

6. OBJECTIVES OF THE POLICY MANUAL

6.1. 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 the **Annexure A** of this policy.

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

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

6.4. Appointing Information Officers to ensure respect for and to promote, enforce and fulfil the rights of Data Subjects referred to in **Annexure A**.

6.5. 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 a loss in revenue where it is found that the personal information of data subjects has 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.

7. DEFINITIONS/TERMINOLOGY AND ACRONYMS

7.1 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.
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 and/or when the legal disclosure of such information to a third party has to be considered.
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. Chabot's 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	A "certified copy" is a copy of an official primary document that has on it an endorsement or a 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 GDE 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 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 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 or 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/caregiver to the School.

Term	Explanation
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 or deleting a record or document or personal information or transferring it into archival custody.
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, electronic information or any other document stored on a database 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 another 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 GDE.

Term	Explanation
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 or tablet or cell phone / Wi-Fi / smartphone / smartwatch which is stored in the network or in / on the recipient's terminal / handheld / portable / digital / electronic equipment until it is collected or 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 / smartphone / smartwatch.
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.
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 a 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 metadata (background and technical information in respect of 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 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.

Term	Explanation
File Plan	A pre-determined classification plan by which records / documents / information is 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. 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 c) a file plan.
Board of Governors	Means the governing body of the School as appointed according to the schools constitution.
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.
Information Matching programme	a) An information matching programme is a comparison, whether manually or by means of any electronic or another 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 supply 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.

Term	Explanation
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 / After Care and/or Grade R Centre.
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 BOG.
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 Gauteng 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, smartwatches 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 does 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.
Personal Information	Means information relating to an identifiable, living, natural person, and where it is applicable and 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 another 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;

Term	Explanation
	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.
Public Body	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.

Term	Explanation
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 another 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 another 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.
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 another legal instrument on behalf and for such natural or legal person.

Term	Explanation
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 the 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 McAuley House school is a school which enrolls learners in one or more grades from grade R to grade twelve.
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 include any form of a 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, 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 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/handheld electronic device.

Term	Explanation
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."*

7.2 Acronyms

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

8. APPLICATION AND SCOPE OF THE POLICY

8.1. At McAuley House School we are committed to protecting the privacy of data subjects and to ensure that their personal information is collected and used properly, lawfully and transparently.

8.2. The BOG and the Principal of the school are ultimately responsible for ensuring that information security is properly managed. The Information Officer, (name), 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 BOG, staff and parents where applicable.
e. The Board of Governors, 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.

8.3. The Information Officers and staff are responsible for adhering to this policy, and for reporting any security breaches or incidents to the Information Officer.

8.4. 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.

8.5. This policy applies to personal information collected by the School in connection with the services it offers. This includes information collected offline through the school's telephone lines and 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.

8.6. 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 BOG and Members of the SMT are required to review procedures in their areas to ensure compliance with this Policy Manual and POPIA as part of the annual planning process of the School.

8.7. This policy does not apply to:

a. information collected by third party websites, platforms and/or applications ("Third Party Sites") which the school/BOG/SMT 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. Which has been de-identified;
f. 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;
h. 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.

8.8. This policy impacts upon the School's work practices and data 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.

9. LEGISLATIVE FRAMEWORK

9.1. Constitution of the Republic of South Africa, Act 108 of 1996.
9.2. South African Schools Act, Act 84 of 1996.
9.3. National Regulations for Safety Measures at Schools, GN 1040 of 2001, as amended.
9.4. The Protection of Personal Information Act no 4 of 2013, as amended.
9.5. South African Council of Educators Act, 2000(Act No. 31 of 2000), as amended.
9.6. Public Service Act, 1994, as amended.
9.7. General Notice 6903 of 2000 as amended, Misconduct of Learners at Public Schools and Disciplinary Proceedings.
9.8. General Notice 1040 of 12 October 200, as amended, Regulations for Safety Measures at Public Schools.
9.9. National Health Act, 2003 (Act No 61 of 2003), as amended and related regulations.
9.10. School Education Act, 1995 (Act 6 of 1995), as amended.
9.11. General Notice 1189 of 2012, Regulations on Domestic and International Tours for Learners at Public Schools, 2012.
9.12. Electronic Communications and Transactions Act, 25 of 2002.
9.13. Financial Intelligence Centre Act, Act 38 of 2001, as amended.
9.14. Compensation for Occupational Injuries and Diseases Act, Act 130 of 1993, as amended.
9.15. Basic Conditions of Employment Act, Act 75 of 1997.
9.16. Employment Equity Act, Act 55 of 1998.
9.17. Labour Relations Act, Act 66 of 1995 and Codes of Good Practice.
9.18. Unemployment Insurance Act, Act 63 of 2002.
9.19. Tax Administration Act, Act 28 of 2011.
9.20. Income Tax Act, Act 58 of 1962.
9.21. Skills Development Levies Act, Act 9 of 1999.
9.22. Securities Services Act, Act 36 of 2004.
9.23. The Control of Access to Public Premises and Vehicles Act 1985 (Act No. 53 of 1985), including regulations made under it ("the Public Premises Act").
9.24. General and Further Education and Training Quality Assurance Act.
9.25. Regulations pertaining to POPIA.
9.26. Umalusi Policy and Criteria.
9.27. National Archives and Records Service of South Africa Act, (Act No 43 of 1996), as amended.
9.28. Guidance Notes on the Processing of Personal Information in the Management and Containment of Covid-19 Pandemic in Terms of the Protection of Personal Information Act 4 of 2013 issued by the Information Regulator of South Africa.
9.29. National Education Policy Act, 1996, Act 27 of 1996, as amended.
9.30. The Criminal Procedure Act, Act 51 of 1977.
9.31. The Films and Publications Act, Act 65 of 1996, as amended.
9.32. Employment of Educators Act, 1998, Act 76 of 1998, as amended.
9.33. Regulation of Interception of Communications and Provision of Communication-Related Information Act, Act 70 of 2002.
9.34. Government Notice 487 dated 6 June 2011 - SC006: Dictionary of Education Concepts and Terms published by the Minister of Basic Education.
9.35. Copyright Act, Act 98 of 1978.
9.36. Short Term Insurance Act, Act 53 of 1998.

10. RELEVANT POLICIES AND PROVINCIAL CIRCULARS

10.1. School Health and Safety Policy.
10.2. Admission Policy of the School.
10.3. Language Policy of the School.

Initialled by Chairperson of the SGB and the Principal _____

10.4. Religion Policy of the School.
10.5. Code of Conduct for Learners and related rules and policies of the School.
10.6. Extra Mural and Sports Policy of the School.
10.7. Transport Policy of the School.
10.8. Asset Register of the School.
10.9. COVID-19 Protocol and Anti-Stigmatisation Policy of the School.
10.10. HIV/AIDS, TB and STI's Policy of the School.
10.11. Domestic and International Tours Policy of the School.
10.12. Privacy Policy of the School.
10.13. School Social Media Policy.
10.14. School CCTV Policy.
10.15. Code of Conduct for Parents and Visitors of the School.
10.16. Personnel Administrative Measures.
10.17. SACE Code of Conduct and the Code of Conduct for Public Servants.
10.18. Contractual obligations of employees employed by the BOG.
10.19. GDE Memorandum – Requirements for Storage of Examination Materials at the District Offices and Examination Centres - 2014

11. POLICY STATEMENTS

11.1. Key Principles of the Policy Manual

11.1.1. 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.

11.2. Commitment to the Principles of POPIA

11.2.1. 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 during induction, or through training programmes, of their responsibilities under the terms of this Policy and POPIA.

11.3. The School is a Private Body

11.3.1. As it is not viewed as a part of the State it has independent powers as assigned to the BOG and the School Principal and SMT.

11.3.2. Exercising a power or performing a duty in terms of the Constitution of South Africa and a provincial constitution.

11.4. The Principles of Compliance

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

11.5. Privacy Policy and Privacy Notice

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

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

11.6. Specific Purpose Collection of Information

11.6.1. 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.

11.7. Rights of Data Subjects

11.7.1. 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.

11.7.2. The rights are as follows:

a) 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 its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22 of POPIA;

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

c) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24 of POPIA;

d) to object, on reasonable grounds relating to his, her or its particular situation to the

processing of his, her or its personal information as provided for in terms of section 11(3)(a) of POPIA;

e) to 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 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;

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

g) 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;

h) 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

i) 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.

11.8. A Word of Caution to Parents/Guardians/Caregivers

11.8.1. 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, which means the parent and the child also have a responsibility to protect the child's 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.

11.8.2. Parents and learners must understand and use the privacy tools on any website or app that the School or 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 to be shared with others, including law enforcement, the school, tertiary institutions and current or future employers).

11.9. Processing of Information by using Automated and Non-automated Means

11.9.1. 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.

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

11.10. General Description of Information Security Measures

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.

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

11.11.1. 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.

11.11.2. 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.

11.11.3. A brief overview of each condition is as follows:

11.11.3.1. 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.

11.11.3.2. 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 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.

11.11.3.3. 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.

11.11.3.4. Condition 4: Further Processing Limitation

1. Conditions 2 and 3 are not 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 of 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.

11.11.3.5. Condition 5: Information Technology or Quality

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

11.11.3.6. 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 don't collect information.
    c. The source of the School’s information
    d. The School’s physical 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 form a data subject is voluntary or mandatory.
    g. What will happen if the data subjects don’t provide their data to the School as requested?
    h. The relevant legislation that allows for data collection from data subjects.
    i. These 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.

11.11.3.7. 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 or authorisation of the School and consider the information to be confidential. Any other (third) parties who process the 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 (See Annexure for example of a log).
    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 with the password or screen finger scan 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, 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.

11.11.3.8. 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.

11.12. Data of Children

11.12.1. The School may not process children's personal information unless:
   a. The School has the consent of a "competent person" (parent/guardian/caregiver/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.

11.12.2. 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.

11.13. Access and Security to Information/Records

11.13.1. Records in all formats, shall at all times be protected against unauthorised access and tampering to protect their authenticity and reliability as evidence of the business of the School.

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

11.13.3. 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 BOG.

11.13.4. 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.

11.13.5. Personal information shall be managed in terms of the policy and POPIA.

11.13.6. 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.

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

11.13.8. Records storage areas shall at all times be protected against unauthorised access. The following shall apply:

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

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

11.13.11. The School's Access to the safes and the walk-in safe and key controls policy will be adhered to.

11.13.12. 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.

11.13.13. 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.

11.14. Performing a POPIA GAP Analysis and Risk Assessments

11.14.1. 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 are deficient.

11.14.2. The gap analysis is unique to the School. But 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.

11.14.3. POPIA's security requirements require the Information Office of the School to take necessary measures for protecting the School's information. The request is broad, but it is meant to be. The School has to take further steps to protect its banking details and other protected personal information than just that of a database consisting of only email addresses or information stored electronically on SA SAMS or similar programmes such as Principal Primary.

11.14.4. 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.

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

11.14.6. The gap analysis can reveal where the School has weaknesses when it comes to protecting the personal data it collects, stores and uses.

11.14.7. 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.

11.14.8. 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.

11.14.9. 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 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. Do the School have processes in place to dispose of private data after use?

11.15. Drafting New Policies and Update Existing Documents

11.15.1. 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.
c. Incident Response Policy for data breaches or any other matters related to personal data.
d. An Information Manual,
e. Reporting Procedures.

11.15.2. 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.

11.16. The School's Compliance Management System

11.16.1. 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.

11.17. Consent to Process Personal Information

11.17.1. In terms of POPIA, a "Responsible Party" (in this case the school) has a legal duty to process a "Data Subject's" personal information (in this case the personal information and related details of a parent/legal/guardian/caregiver and/or any enrolled learner and/or any employee of the school and the GDE and/or any other person) in a lawful, legitimate and responsible manner.

11.17.2. 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.

11.17.3. 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.

11.18. Signature of any document and the Purpose of a Signature on a document

11.18.1. 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 pout and

Initialled by Chairperson of the SGB and the Principal _____

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 BOG or a company, however, the representative must be authorised in writing or by a resolution or a power of attorney to do so.

11.19. Witnessing documents

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

11.19.2. 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.

11.19.3. 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).

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

11.19.5. 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.

11.20. Steps to Correctly Witness a Signature

11.20.1. 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 are 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.

11.21. Common Acts of POPIA Non-Compliance:

11.21.1. 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 the incorrect recipient including on any groups on any social media application or platform.
c. Insecure webpage (including hacking).
d. Loss or theft of an 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 the webpage.
i. Verbal disclosure without permission or carelessly done.
j. Insecure disposal of hardware.
k. Sending confidential data by e-mail/Apps that are 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 unsecured links.

11.22. POPIA and E-mail Usage

11.22.1. If it is needed, each Staff member within the School is provided with a school email account to assist with their work for the School. This account is the primary way that staff members will communicate with parents and other colleagues and other agencies and entities.

11.22.2. Email account holders must comply at all times with this Policy.

11.22.3. The email account of a staff member, and any information contained in it including content, headers, directories and email system logs, remains the property of the School.

11.22.4. Usage of the school email system is mainly for school, academic and professional purposes.

11.22.5. Incidental use of an e-mail account for personal purposes is allowed and is subject to the same policies and regulations as official use. However, systematic use on behalf of individuals or organisations that are not associated with the School or its business is not allowed.

11.22.6. 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.

11.22.7. 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 the information stored on any network device belonging to the School.

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

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

11.22.10. Any defamatory or careless remarks can have very 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.

11.22.11. To prevent computer viruses being transmitted through the network, care must be taken when dealing with suspect e-mails and attachments of unknown origin are received. Suspect e-mails should be deleted immediately and never forwarded to other Users.

11.22.12. E-mail users must be aware of the use of dangerous code by hackers and other outside parties which refers to any computer programme that causes destruction or harm and has been programmed in such a way with the malicious intent of the content of a computer or other electronic communication device. Dangerous Code is classified as file infector viruses, system or boot record viruses and macro viruses. It must be noted that viruses can either be decimated or "contracted" by the exchange of various media or by the receipt in an e-mail from a source that is unknown or spam. Effective anti-virus software will normally indicate such e-mails.

11.22.13. Staff and learners 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.

11.22.14. 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 immediately.

11.23. POPIA and Bulk E-mail

11.23.1. From time to time the School authorities may wish to communicate with parents via bulk email.

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

a. Staff and members of the BOG 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.

11.23.3. 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/e-mails 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 the 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. 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.

11.23.4. E-mail messages must be kept as short as possible and must contain only text:
a. Images, logos, 'watermark' backgrounds, etc. are not permitted since they greatly increase the size of a message.
b. Emails to the list must as far as possible not include any attachments. Where there is a need to provide staff with copies of reports, forms etc., these should be made available on the school web to which only staff members may have access and a link to the document included in the message.
c. In general, messages should be sent only once. Exceptionally, official reminders and security/safety-related messages may be repeated.

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

11.24. POPIA and Internet Usage and Connections

11.24.1. 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.

11.24.2. 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 BOG.
e. To provide lists or information about the School or the School's staff, parents/ guardians/caregivers/agents/contractors, BOG members or learners to others and/or to send other confidential information without approval.

11.25. POPIA and Personal Websites

11.25.1. The School recognises that from time to time staff will set up websites, blogs or wikis that, while related to their academic or professional disciplines, are personal sites and not formal School Sites.

11.25.2. 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.

11.25.3. 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 BOG.

11.25.4. 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.

11.25.5. On personal websites, staff members are required to identify views expressed as their own and that the staff member does not hold him-/herself out as representing the School. If an employee of the school identifies 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.

11.26. Retention of Personal Information Records

11.26.1. 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 PII the school shall retain the records to the extent that it is needed or required by law for a shorter period.

11.27. Records that cannot be found or do not exist or believed not to exist

11.27.1. 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.

11.28. Scanned documents

11.28.1. 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.

11.28.2. 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.

11.29. Monitoring and Implementation of the Policy

11.29.1. The BOG, the SMT, 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.

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

11.30. Operating Controls

11.30.1. The BOG, the Principal, and SMT 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.

11.31. Duty to Report a Vulnerable Child in Need of Protection

11.31.1. 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 might be at risk if they have reasonable grounds to suspect that a child is in need of protection and complete a Form 22.

11.32. Notifying Parents of Harm to Learners

11.32.1. The GDE 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 BOG 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.

11.33. Occupational Health and Safety

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

11.34. Certified Copies

11.34.1. Certified copies 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's 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.

11.34.2. 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.

11.34.3. 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.

11.34.4. To request certification of a copy of a document the data subject has 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.

11.34.5. 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.

11.34.6. 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.

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

11.35. School Photographs/Images/Videos of Learners

11.35.1. 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.

11.35.2. The School is permitted to collect personal information, including photographs, where it is necessary to 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).

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

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

11.35.5. 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.

11.35.6. The permission of parents may be obtained for the use of photographs for other purposes such as annual photo's for parents or the website, the media or promotional purposes, provided that children at risk are not shown or their images pixelated.

11.35.7. Images and any other videos of learners on the school's website must be disabled so that it cannot be copied or downloadable

11.36. BOG Employees' Information

11.36.1. Each appointed employee of the BOG 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.

11.36.2. Each BOG 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.

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

11.37. CCTV

11.37.1. 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 the 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.

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

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

11.38. Entry to the School Grounds by Parents and Visitors

11.38.1. The School and BOG 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 premise in the principal's discretion.

11.39. Bots

11.39.1. 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.

11.40. Direct Marketing by Means of Unsolicited Electronic Communications

11.40.1. 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.

11.40.2. Direct marketing is PROHIBITED unless the school has obtained 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.

11.40.3. 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.

11.40.4. Any communication for the purpose of direct marketing from the School must contain:

11.40.4.1. 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

11.40.4.2. The address or other contact details to which the recipient may send a request to opt-out.

11.40.5. 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.

11.41. POPIA Complaints Procedure

11.41.1. Complaints may be filled via email to the School at email: principalh@mcauleyhouse.co.za

11.42. Destruction of Documents

11.42.1. 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.

11.42.2. 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.

11.42.3. 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.

11.42.4. 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.

11.43. Disciplinary Action

11.43.1. 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 reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

11.43.2. In the case of ignorance or minor negligence, the School will undertake to provide further awareness training to the employee.

11.43.3. Any gross negligence or the willful mismanagement of personal information will be considered a serious form of misconduct for which the School may summarily dismiss the employee.

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

11.44. Personal Information No Longer Personal Information

11.44.1. 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.

11.45. Encryption of Personal Information

11.45.1. Encryption is a key technical measure for securing school data and the first line of defence, and all electronic information must have encryption and passwords to access personal information. Encryption is very important and is a key aspect of complying with POPIA.

11.46. Information held in "THE CLOUD" to comply with POPIA

11.46.1. 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.

11.47. Data Portability

11.47.1. It 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.

11.47.2. 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.

12. SHORT TITLE

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

13. AMENDMENTS

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

14. APPROVAL

Recommended by Principal	**Mr. R Davis**	**Signature:**	
Date:			
Approved by BOG Chairperson	**Mr. R Adams**	**Signature:**	
Date:			
Verification by GDE		**Signature:**	
Certified by		**Signature:**	
Date:			

SCHOOL STAMP

Initialled by Chairperson of the SGB and the Principal _____

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. Learners' 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 an LSEN number allocated by the GDE and/or account number.
   v. Gender.
   vi. Race.
   vii. Physical address and contact details.
   viii. Medical and health information and, where necessary, a 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:
   xiii. Birth certificate;
   xiv. ID documents;
   xv. Inoculation certificate;
   xvi. Report cards from a previous school;
   xvii. Study and asylum permits;
   xviii. If applicable, change of name/surname certificate and new ID details.

c. Learner profiles and documents in profiles.
d. Transfer Card (where applicable from a 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 psychosocial 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 GDE/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

1. 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.
    a. Financial record of school fee account:
        i. Ledger account.
        ii. Statement of account.
        iii. Receipts.
        iv. Journal entries.
        v. Correspondence and documents.
    b. 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 the income of the 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 a child is in care.
    c. Compensation of school fees.
    d. Correspondence with parents.
    e. CCTV footage of parents.

3. EMPLOYEES EMPLOYED BY THE SCHOOL

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 copies of Driver's license – Professional Driving Permits.
xxii. Photographs and copy of access card.
xxiii. Police Clearance Certificate.
xxiv. Payslip registers.
xxv. Leave application forms.
xxvi. Claims expenses from School.

b. Personal Information on 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. 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. Payslips.
i. Payslip 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.

5. 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.

6. 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).

Initialled by Chairperson of the SGB and the Principal _____

7. BOARD OF GOVERNORS AND BOG COMMITTEES

a. Personal information of all BOG members.
b. Contact details/e-mails/cell phone numbers and landline numbers.
c. Constitution of the BOG.
d. Budgetary Information.
e. Correspondence – general and specific.
f. Minutes of all meetings.
g. Agendas of Meetings.
h. Attendance Registers.
i. School Policies and Guidelines.
j. Strategic Planning documents.

8. NATIONAL GOVERNMENT DEPARTMENTS, THE DEPARTMENT OF BASIC EDUCATION AND THE GAUTENG 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 a loan, extend, lease etc.
q. Correspondence hard copy and electronic messages.

9. 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 the new school or after leaving school.
e. Copies of Transfer Cards.
f. Matric certificates/last record of attendance/report cards.

10. SPONSORS/DONORS/SUPPORTERS

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

11. ADVERTISERS

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

Initialled by Chairperson of the SGB and the Principal _____

12. SPORTING BODIES/AFFILIATIONS/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.

13. 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.

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

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

15. STATUTORY BODIES - SARS – DEPARTMENT OF LABOUR- SETA'S

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

16. SCHOOL AUDITORS

a. Personal Information details.
b. Letter of appointment from the BOG.
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.

17. 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

18. BANKING INSTITUTIONS

a. Personal information details.
b. Correspondence who has signing authority/EFT authority.
c. Contact details of banking representative.

Initialled by Chairperson of the SGB and the Principal _____

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 repayments and transactions.
j. Debit card machine records and transaction slips.
k. Banking fees records.

19. ATTORNEYS / DEBT COLLECTORS /LEGAL COUNSEL

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

20. OUTSOURCED CLEANING SERVICES AND OTHER SERVICES

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

21. EDUCATIONAL INSTITUTIONS (UNIVERSITIES/OTHER TERTIARY INSTITUTIONS)

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

22. INFORMATION TECHNOLOGY

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

23. 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. Academic Policy General
    ii. Academic and Assessment Policy HS
    iii. Academic and Assessment Policy PS
    iv. Admissions Policy
    v. Anti- Bullying Policy
    vi. Bursary/ Financial Assistance Policy
    vii. Bursary/ Financial Assistance Declaration
    viii. Career Guidance Policy
    ix. Catholic School Code Of Ethics Determining Relationships Between Schools
    x. Computer Centre Code of Conduct
    xi. Data Management Policy
    xii. Data on Server Policy

Initialled by Chairperson of the SGB and the Principal _____

xiii. Discipline Policy High School
xiv. Discipline Policy Primary School
xv. Drug Policy
xvi. Excursion Policy
xvii. Educator Succession Policy
xviii. Finance Policy
xix. Fixed Asset Management Policy
xx. General School Policy
xxi. Grade 9 Subject Choice Policy
xxii. Health and Safety Policy
xxiii. Infectious Diseases Policy (Replaced Aids Policy)
xxiv. IQMS Policy
xxv. Learner Support Policy
xxvi. Learning Programme Development, Delivery and Evaluation Policy
xxvii. Pastoral Care :Policy
xxviii. Policy Creation and Review Policy
xxix. Policy for Evaluation
xxx. Policy for Evaluation Tool
xxxi. Procurement of Teaching and Learning Materials
xxxii. Pregnancy Policy
xxxiii. Pupils Code of Conduct HS
xxxiv. Pupils Code of Conduct PS
xxxv. Recruitment Policy
xxxvi. Review of Policies Policy
xxxvii. Sexual Behaviour Policy
xxxviii. Staff Social Media Policy
xxxix. Staff Code of Conduct
xl. 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. Organogram 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

POPIA - RECORDS DISPOSAL REGISTER

YEAR	
DEPARTMENT	

DATE	RECORD TO BE DISPOSED	RECORD FOR DISPOSED	EMPLOYEE NAME	IO APPROVAL FOR DISPOSAL	DEPARTMENT HEAD ATTEST TO DISPOSAL

PERSONAL INFORMATION LOG

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

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