AUBURN HOUSE SCHOOL

PROTECTION OF PERSONAL INFORMATION ACT

POLICY

PROTECTION OF PERSONAL INFORMATION POLICY[1]

A. INTRODUCTION

1. Background

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy, the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. The Protection of Personal Information Act ("POPIA") is South Africa's data protection law.[2]

2. Purpose

POPIA is intended to promote the protection of personal information processed by public and private bodies and establish minimum requirements for the processing of personal information in a context-sensitive manner. This Policy is intended to facilitate the responsible processing of personal information received by the School in accordance to the right to privacy of data subjects (pupils, parents, employees and other stakeholders).

3. Applicability

As an educational institution, Auburn House School ("School") is necessarily involved in the processing of the personal information of pupils, parents, employees and other stakeholders for administrative and other purposes. In accordance with the provisions of POPIA, Auburn House School is committed to effectively managing, collecting, handling and disposing of personal information.

4. Details of the School:

Postal address of the School:	3 Auburn Road, Kenilworth, Cape Town 7701
Street address of the School:	3 Auburn Road, Kenilworth, Cape Town 7701
Telephone number of the School:	021 7977872
E-mail Address of the School	info@auburnhouse.co.za
Information Officer at inception of Policy: Contact in writing:	Tasnim Rylands tasnimr@auburnhouse.co.za
Deputy Information Officer at inception of Policy Contact in writing:	Megan Stead megans@auburnhouse.co.za Melanie Vaughan melaniev@auburnhouse.co.za

5. Objectives

i. 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.

ii. Protecting the School's records and information in order to ensure the continuation of the day to day running of the school.

---

[1] These Guidelines are based on the ISASA POPIA Guidelines available on the ISASA website.
[2] A copy of POPIA can be obtained here: https://popia.co.za/act/.

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

iv. Appointing Information Officers to ensure respect for and to promote, enforce and fulfil the rights of Data Subjects.

v. 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; and

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.

6. DEFINITIONS

The following definitions in the POPIA are key in determining what activities undertaken by education institutions will be affected by the Policy:

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.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data Subject	This refers to the natural or juristic person to whom personal information relates, such as individual pupils, parents, employees or a company that supplies the school with services, products or other goods.
De-Identify	Means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.
Direct Marketing	Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: • promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or • requesting the data subject to make a donation of any kind for any reason.
Filing System	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.
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.
Information Officer	The Information Officer is responsible for ensuring the organisation's compliance with POPIA but it is ultimately the Head of the school who is responsible for ensuring that the Information Officer's duties are performed. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties.
Operator	An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the organisation and whose service requires access to personal information of pupils, parents and employees. (When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.)
Personal Information	Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning: • race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; • information relating to the education or the medical, financial, criminal or employment history of the Person; • any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; • the biometric information of the person; • the personal opinions, views or preferences of the person; • 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; • the views or opinions of another individual about the person; or • 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.
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.
Processing	The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes: • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; • dissemination by means of transmission, distribution or making available in any other form; or • merging, linking, as well as any restriction, degradation, erasure or destruction of information.
Record	Means any recorded information, regardless of form or medium, including: • writing on any material; • information produced, recorded or stored by means of any recording equipment, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; • label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; • book, map, plan, graph or drawing; or • photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.
Re-Identify	In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.
Responsible Party	The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. The school is the responsible party.

B. POLICY APPLICATION

This policy and its guiding principles apply to all sections of Auburn House School, ie Pre-primary 3-6 years, Junior Primary 6-9 years and Senior Primary 9-12 years.

1. Who is Responsible for Compliance?

i. The Head of School

The Head of School is automatically deemed to be the Information Officer in accordance with the provisions of POPIA but may delegate their duties to a Deputy Information Officer(s). Duties of the Information Officer are as follows:

a. the encouragement of compliance by the school with the conditions for the lawful processing of personal information;

b. dealing with requests made to the school pursuant to POPIA;

c. working with the Information Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA (Prior Authorisation) in relation to the School;

d. ensuring that a compliance framework is developed, implemented, monitored and maintained;

e. monitoring and implementing Codes of Conduct issued by the Information Regulator; and

f. otherwise ensuring compliance by the school with the provisions of POPIA.

ii. All employees

Both permanent and temporary staff, staff working on a contract basis for the School, coaches, volunteers and others who are authorised to access personal data held by the School.

iii. All contractors, suppliers and other persons acting on behalf of the organisation.

2. Compliance with this Policy

The Information Officer, Deputy Information Officer(s), and staff are responsible for adhering to this Policy, including:

i. the development and upkeep of this policy;

ii. ensuring this policy is supported by appropriate documentation, such as procedural instructions.

iii. ensuring that documentation is relevant and kept up to date;

iv. ensuring this policy and subsequent updates are communicated to the Board of Governors, staff and parents where applicable;

v. ensuring that the school's Board of Governors, the School's employees, volunteers, contractors, suppliers and any other persons acting on behalf of the School have familiarised themselves with this Policy's requirements and undertake shall comply with the stated processes and procedures; and

vi. reporting any security breaches or incidents to the Information Officer.

3. Scope of Policy

This Policy applies to personal information collected by the School in connection with the services it offers. This includes information collected by the School, at its premises, 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. 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.

C. THE PRINCIPLES OF LAWFUL PROCESSING OF PERSONAL INFORMATION

The School undertakes to lawfully process personal information by ensuring compliance with the following eight guiding principles:

1. To assign responsibility to designated persons for lawful processing of information

The School must assign and register the Information Officer and Deputy Information Officers who will ensure that personal information is collected and processed in accordance with POPIA. These persons will oversee and manage the School's compliance with POPIA and will furthermore handle all requests made by learners, parents, staff and all relevant stakeholders, for access to information.

The designated persons will ensure that the School takes appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the responsibilities outlined in this policy.

2. To only collect data needed for legitimate purposes

Personal information must be collected for a specific, explicitly defined, and lawful purpose. Therefore, the School will always determine the purposes for which the personal information was collected.

2.1 To ensure it has a legal basis for processing (Justification)

Once the purpose for processing the personal information has been determined, the lawfulness of the processing activity must be assessed. All processing activities must have a legal basis. POPIA provides several justifications for processing activities:

i. Personal information may be processed to conclude or perform in terms of a contract;

ii. Personal information may be processed to comply with an obligation imposed by law;

iii. Personal information may be processed to protect a legitimate interest of the data subject;

iv. Personal information may be processed to ensure proper performance of a public law duty by a public body;

v. Personal information may be processed to ensure the legitimate interest of the responsible party or of a third party;

vi. Personal information may be processed with the consent of the data subject or a competent person where the data subject is a child. Consent must be voluntary, specific, explicit, informed and the data subject has the right to withdraw consent at any time.

3. To use the information in a way that matches the purpose of collection

The processing must be necessary to fulfil the purpose of the collection and it must be the least invasive way to achieve that purpose. Any further processing of personal information (for a secondary purpose) by the School must be upon the consent obtained from the relevant Data Subject.

4. To ensure that the information is accurate and regularly updated

The School must ensure that the personal information being processed is regularly updated. This means that the school must maintain the quality of the personal information and as such all personal information must be kept reliable, accurate, up-to-date and relevant to the purposes for which it was collected.

5. **To ensure that information is processed in a fair and transparent manner**

   Schools are to ensure that Data Subjects are aware of the specific personal information held about them by the School and the purpose to which the information is being collected.

6. **Information Security**

   The School must take reasonable security steps to protect the integrity of the information and safeguard personal information collected by it against:

   i. damage;

   ii. loss;

   iii. loss of access;

   iv. unauthorised destruction;

   v. unauthorised access; and

   vi. unauthorised use.

7. **Store the information only as long as required**

   The retention of all personal information by the School will be guided by all relevant and applicable laws, regulations and policies. Furthermore, all personal information may only be kept for as long as it is required to fulfil the purpose for which it was collected.

   The School will ensure that all personal information is destroyed, deleted or de-identified as soon as it is becomes irrelevant, outdated and/or upon the request of a Data Subject. This process shall render the data irretrievable.

8. **Uphold data subjects' rights by providing access and corrections to the information**

   The School is to ensure that there are accessible processes in place to ensure that properly identified data subjects have the right to access related personal information and/or request the correction or deletion of any personal information held about them that may be inaccurate, misleading or outdated.

D. PROCESSING SPECIAL PERSONAL INFORMATION AND THE INFORMATION OF CHILDREN

1. **The School undertakes to lawfully process 'special personal information'**

   Special personal information is information that relates to:

   i. religious beliefs;

   ii. philosophical beliefs;

   iii. race;

   iv. ethnicity;

   v. trade union membership;

   vi. political persuasion;

   vii. health;

   viii. sex life;

   ix. biometric information; or

x. allegations of criminal behaviour or information that relates to criminal proceedings; or

xi. Personal information about children is also a special category of information.

For the processing of 'special personal information' to be lawful, the processing must be justified on one of the grounds discussed in part C, above, and a ground set out in this section below.

2. General justifications for the processing of special personal information:

i. The establishment, exercise or defence of a right in law;

ii. International public law;

iii. Historical, statistical, or research purposes;

iv. The information has deliberately been made public by the data subject;

v. The data subject gave consent; and

vi. The information may be processed for health reasons.

3. Processing the information of children must be justified

Personal information of children may be processed by the School only if:

i. the parent or guardian consents to the processing of the child's personal information;

ii. processing is necessary for compliance with an obligation imposed by law;

iii. processing is necessary to comply with an obligation imposed in terms of international public law;

iv. processing is for historical, statistical, or research purposes; or

v. personal information was deliberately made public by the child with the consent of the child's parent(s) or guardian(s).

E. DATA SUBJECT PARTICPATION

1. Rights of the Data Subject

In order to ensure that Data Subjects are made aware of the rights conferred upon them by POPIA the School notes for the purposes of this Policy that Data Subjects have, amongst others, the right to:

i. be notified that personal information about them is being collected;

ii. request access to, the correction of, or the deletion of any Personal Information held by the school using the form attached hereto as Annexure "A" to this Policy;

iii. withdraw consent to process their personal information in terms of the Form attached hereto as Annexure "B";

iv. lodge a complaint concerning the processing of their personal information in terms of the Form attached hereto as Annexure "C";

v. object, on reasonable grounds, to the processing of their personal information;

vi. object to the processing of their personal information at any time for purposes of direct marketing;

vii. be notified that their personal information has been accessed or acquired by an unauthorised person;

viii. submit a complaint to the Information Regulator regarding the alleged interference with the protection of their personal information; and

ix. institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

2. Processes to vindicate the rights of Data Subject

The School will uphold the rights of the Data Subject by ensuring that it:

i. does not collect data unnecessarily;

ii. implements this Policy in respect of processing personal information;

iii. does not retain records of personal information longer than it is necessary for achieving the purpose for which the personal information was collected, or as may be prescribed in terms of a law or contract, or with the consent of the data subject;

iv. trains staff on the obligations imposed by POPIA when they process personal information;

v. ensures that personal information is securely stored;

vi. has complete control over personal information kept at the school;

vii. keeps a catalogue system to assist the school to address requests for access to personal information by Data Subjects;

viii. destroys and / or deletes Personal Information this will be conducted in a manner that prevents its reconstruction or reidentification;

ix. informs Data Subjects about the use of a CCTV on the premises;

x. informs the Data Subject if it collects personal information for marketing or advertising purposes and provides an opportunity for them to object;

xi. In the case of an access breach to the personal information under the control of the School the School will notify the Data Subject and the Information Regulator in writing as soon as reasonably possible after the discovery of the access breach to the personal information via either:

a) mail at the last known physical or postal address;

b) e-mail to the last known e-mail address;

c) publishing a notice on the school website; or

d) publishing a notice in the news media, and

xii. where applicable, Auburn House School will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

3. Rights of the School

Please note that the School may lawfully process personal information without obtaining consent from a Data Subject if the processing of the personal information:

i. is necessary for pursuing the legitimate interest of the school or of a third party to whom the information is given;

ii. protects a legitimate interest of a Data Subject;

iii. is necessary to conclude or perform a contract to which a Data Subject is a party; or

iv. complies with an obligation imposed by law.

F. SECURITY SAFEGUARDS

The school, in order to ensure that all personal information is adequately protected, shall takes steps to:

i. implement security controls in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction;

ii. apply Security measures in a context-sensitive manner;

iii. continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the school's IT network;

iv. ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals;

v. ensure that all new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information;

vi. ensure that all existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses; and

vii. ensure that all the school's operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

G. SPECIFIC DUTIES AND RESPONSIBILITIES OF SCHOOL'S POPIA TEAM

1. Information Officer (and/or Deputy Information Officer/s)

The school's Information Officer (or delegated Deputy Information Officer/s) is responsible for:

i. keeping the Management Team and/or Board of Governors and/or Board of Trustees of the School updated about the School's responsibilities under POPIA;

ii. continually analysing POPIA regulations and/or notices issued by the Information Regulator in order to align these with this Policy and procedures thereto;

iii. ensuring that POPIA Audits are scheduled and conducted on a quarterly basis;

iv. ensuring that the School has accessible processes in place makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to the School;

v. approving any contracts entered into with operators, employees and other third parties which may have an impact on the Personal Information held by the School;

vi. oversee the amendment of the School's employment contracts and other service level agreements;

vii. ensure that employees and other persons acting on behalf of the School are fully aware of the risks associated with the processing of personal information and that they remain informed about the School's security controls.

viii. organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the School;

ix. addressing employees' POPIA related questions;

x. addressing all POPIA related requests and complaints; and

xi. working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

2. SMT - IT

The school's SMT is responsible for:

i. ensuring that the school's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards;

ii. ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services;

iii. ensuring that servers containing personal information are sited in a secure location, away from the general office space;

iv. ensuring that all electronically stored personal information is backed-up and tested on a regular basis;

v. ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts;

vi. ensuring that personal information being transferred electronically is encrypted;

vii. ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software;

viii. performing regular IT audits to ensure that the security of the school's hardware and software systems are functioning properly;

ix. performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons; and

x. performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the school's behalf. For instance, cloud computing services.

3. SMT - Marketing

The school's SMT is responsible for:

i. approving and maintaining the protection of personal information statements and disclaimers that are displayed on the school's websites, including those attached to communications such as emails and electronic newsletters;

ii. addressing any personal information protection queries from journalists or media outlets such as newspapers; and

iii. where necessary, working with persons acting on behalf of the school to ensure that any outsourced marketing initiatives comply with POPIA.

4. Employees and other persons acting on behalf of the School

Employees and other persons acting on behalf of the school will, during the course of the performance of their services, gain access to and become acquainted with the

personal information of certain pupils, parents, suppliers and other employees. Employees and other persons acting on behalf of the school are required to treat personal information as a confidential business asset and to respect the privacy of Data Subjects in the following manner:

i. employees and other persons acting on behalf of the school may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the school or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties;

ii. employees and other persons acting on behalf of the school must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a Data Subject's personal information;

iii. employees and other persons acting on behalf of the school will only process Personal Information where:

   a) the data subject, or a competent person where the data subject is a child, consents to the processing; or

   b) the processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party; or

   c) the processing complies with an obligation imposed by law on the responsible party; or

   d) the processing protects a legitimate interest of the Data Subject; or

   e) the processing is necessary for pursuing the legitimate interests of the School or of a third party to whom the information is supplied.

Employees and other persons acting on behalf of the school will under no circumstances:

i. process or have access to Personal Information where such processing or access is not a requirement to perform their respective work-related tasks or duties;

ii. save copies of Personal Information directly to their own private computers, laptops or other mobile devices like tablets or smartphones. All personal information must be accessed and updated from the school's administrative system and central database on dedicated servers;

iii. share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure; or

iv. transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the School are responsible for:

i. keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy;

ii. ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created;

iii. ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons;

iv. ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

v. ensuring that where personal information is stored on removable storage media such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

vi. ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet;

vii. ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer;

viii. taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the parent or customer phones or communicates via email;

ix. taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner;

x. undergoing POPIA Awareness training from time to time; and

xi. reporting any suspicious activity, security breach, interference, modification, destruction or the unsanctioned disclosure of personal information, immediately to the Information Officer.

H. POPIA AUDIT

The school's Information Officer will schedule periodic POPIA Audits.

The purpose of a POPIA audit is to:

i. identify the processes used to collect, record, store, disseminate and destroy personal information;

ii. determine the flow of personal information throughout the School. For instance, the transfer of information from one section of the school to another;

iii. redefine the purpose for gathering and processing personal information;

iv. ensure that the processing parameters are still adequately limited;

v. ensure that new data subjects are made aware of the processing of their personal information;

vi. re-establish the rationale for any further processing where information is received via a third party;

vii. verify the quality and security of personal information;

viii. monitor the extent of compliance with POPIA and this policy; and

ix. monitor the effectiveness of internal controls established to manage the School's POPIA related compliance risk; and

x. liaise with line managers in order to identify areas within the School's operation that are most vulnerable or susceptible to the unlawful processing of personal information.

I. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Access to information requests can be made by email, addressed to the Information Officer in a form substantively similar to Annexure "A". Once the completed form has been received, the Information Officer will verify the identity of the Data Subject prior to handing over any Personal Information. All requests will be processed and considered against this Policy. The Information Officer will process all requests within a reasonable time.

J. POPIA COMPLAINTS PROCEDURE

Data subjects have the right to lodge a written complaint with the School in instances where there is any reason to believe that their rights under POPIA have been infringed upon. Auburn House School takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

i. POPIA complaints must be submitted to the school in writing in a form substantively similar to Annexure "B";

ii. where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 3 working days;

iii. the Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days;

iv. the Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner;

v. in considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA;

vi. the Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the School's Data Subjects;

vii. where the Information Officer has reason to believe that the personal information of Data Subjects has been accessed or acquired by an unauthorised person, the Information Officer the affected data subjects and the Information Regulator will be informed of this breach; and

viii. the Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the school's Information Officer within 7 working days of receipt of the complaint;

ix. in all instances, the School will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines;

x. the Information Officer's response to the data subject may comprise any of the following:

a) a suggested remedy for the complaint;

b) a dismissal of the complaint and the reasons as to why it was dismissed; or

c) an apology (if applicable) and any disciplinary action that has been taken against any employees involved; and

xi. the Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.

Where the data subject is not satisfied with the Information Officer's suggested remedies, the Data Subject has the right to lodge a complaint with the Information Regulator.

K. DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA infringement investigation has been finalised, Auburn House 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. In the case of ignorance or minor negligence, the School will undertake to provide further awareness training to the employee. 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. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

i. A recommendation to commence with disciplinary action.

ii. A referral to appropriate law enforcement agencies for criminal investigation.

iii. Recovery of funds and assets in order to limit any prejudice or damages caused.

L. CAUTION TO PARENTS/GUARDIANS/CAREGIVERS

i. 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.

ii. 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).