

ALEXANDRA EDUCATION COMMITTEE

PBO 930-000-698 | NPO 025-968-NPO

PROTECTION OF PERSONAL INFORMATION POLICY

Issued in terms of the Protection of Personal Information Act 4 of 2013 (POPIA)

Version	1.0
Effective Date	3 June 2026
Next Review	3 June 2027
Information Officer	Paul Kevan Channon (Executive Director) — director@alexeducation.org.za
Deputy IO	Bronwynne Viljoen — bron@alexeducation.org.za

CONTENTS

1. Background and Introduction
2. Definitions
3. Scope and Application
4. Lawful Basis for Processing
5. Consent
6. Purpose Limitation
7. Accuracy
8. Data Minimisation
9. Transparency and Processing Notices
10. Security of Personal Information
11. Records Management
12. Retention and Disposal
13. Operators and Third-Party Processors
14. Sharing Personal Information with Third Parties
15. Cross-Border Transfers
16. Direct Marketing and Communications
17. Reporting Personal Information Breaches
18. Data Subject Rights and Requests
19. The Right to Complain
20. Governance
21. Training and Awareness
22. Non-Compliance
23. Version and Amendments
POPIA Compliance Coverage
Schedule A – Data Subject Categories and Processing Purposes
Schedule B – Personal Information Breach Report Form

POPIA Compliance Coverage

The table below maps the key chapters and requirements of the Protection of Personal Information Act 4 of 2013 to the corresponding sections of this Policy, confirming that all material provisions of POPIA applicable to the AEC are addressed.

POPIA Chapter / Requirement	Policy Section(s)	How Addressed
Definitions and Purpose	Section 2	All key POPIA terms defined (consent, data subject, IO, operator, personal information, processing, responsible party, special personal information).
Application Provisions	Section 3	Policy applies to all staff, volunteers, council members and contractors; covers all forms of personal information regardless of medium.
Conditions for Lawful Processing	Sections 4, 5, 6, 7, 8, 9	All eight POPIA conditions addressed: accountability (s20), processing limitation (s21), purpose specification (s13-14), further processing limitation (s15), information quality (s16), openness (s17-18), security (s19), data subject participation (s23-25).
Exemption — Conditions	Section 4	Special personal information provisions addressed; basis for processing race and residence data for bursary eligibility under POPIA s27(1)(a) documented.
Supervision (Information Officer)	Section 20	IO (Executive Director) and DIO appointed and named; roles, responsibilities and contact details documented; annual review obligation noted.
Prior Authorisation	Sections 4 and 13	Special personal information and cross-border transfers assessed; written operator agreements required before processing commences; IO approval required for new processors.
Codes of Conduct	Sections 21 and 22	Mandatory staff awareness training; induction and annual refresher programme; disciplinary consequences for breach of Policy.
Direct Marketing	Section 16	Opt-in consent required for unsolicited marketing; opt-out mechanism in all communications; removal from mailing lists within 14 days of opt-out.
Transborder Information Flows	Section 15	Cloud services assessed annually by IO; operator agreements require equivalent POPIA protections; disclosure maintained in PAIA Manual (s5.7.7).
Enforcement	Sections 18 and 19	Data subject rights procedures in place (confirmation, access, correction, deletion, objection, withdrawal); 30-day response

POPIA Chapter / Requirement	Policy Section(s)	How Addressed
		timeframe; Information Regulator referral pathway provided.
Offences, Penalties and Fines	Section 22	R10 million fine and imprisonment risk noted; staff non-compliance subject to disciplinary action and potential referral to Information Regulator.
General Provisions	Sections 1, 3 and 23	Policy aligned with POPIA and AEC PAIA Manual (May 2026); effective May 2026; next review March 2027; amendments communicated to staff and published on website.

1. Background and Introduction

The Protection of Personal Information Act 4 of 2013 (POPIA), which came fully into force on 1 July 2021, is the primary South African statute governing the collection, use, storage, sharing and destruction of personal information. POPIA gives effect to the constitutional right to privacy and imposes obligations on any organisation that processes personal information about identifiable persons.

The Alexandra Education Committee (AEC or the Organisation) is a non-profit organisation (NPO 025-968-NPO) and Public Benefit Organisation (PBO 930-000-698) registered in South Africa. The AEC processes personal information about learners, bursary applicants, parents and guardians, donors, employees, contractors and other individuals in the course of carrying out its educational and charitable mission. As a Responsible Party, the AEC is bound by the eight information-protection conditions set out in POPIA.

This Policy has been adopted by the AEC to provide clear and practical guidance to all staff, volunteers, council members and contractors on how to handle personal information lawfully, responsibly and in a manner consistent with the Organisation's values and legal obligations. It should be read alongside the AEC's PAIA Manual (updated June 2026) and any processing notices issued from time to time.

2. Definitions

The following terms, as defined in POPIA, are used throughout this Policy:

Term	Meaning
Consent	Any freely given, specific, informed and unambiguous indication of a data subject's wishes by which they signify agreement to the processing of their personal information.
Data Subject	Any identifiable, living natural person (or existing juristic person) whose personal information is processed.
Information Officer (IO)	The Executive Director of the AEC, responsible for POPIA compliance. Currently: Paul Kevan Channon.
Deputy Information Officer (DIO)	Bronwynne Viljoen, designated to assist the IO and act in the IO's absence.
Operator	Any person who processes personal information on behalf of the AEC under a mandate, and not subject to the AEC's direct authority (e.g. an IT service provider or payroll bureau).
Personal Information	Any information relating to an identifiable, living, natural person or juristic person, including name, contact details, identity number, financial information, health information, educational records and any other identifying information.
Processing	Any operation performed on personal information, including collection, storage, retrieval, use, disclosure, erasure or destruction.

Term	Meaning
Responsible Party	The AEC, as the entity that determines the purpose of and means for processing personal information.
Special Personal Information	Race or ethnic origin, religion, health or sex life, criminal behaviour, biometric information, and information about children under 18.

3. Scope and Application

This Policy applies to all personal information processed by the AEC, whether in paper or electronic form, regardless of the medium on which it is held.

It applies to all individuals who process personal information on the AEC's behalf, including:

- Permanent and contract employees;
- Volunteers and interns;
- Council and sub-committee members;
- Operators and third-party service providers acting under mandate from the AEC.

This Policy covers personal information about all categories of data subjects with whom the AEC interacts, including learners and bursary applicants, parents and guardians of minor learners, donors, employees, contractors and other third parties.

This Policy must be read together with the AEC's PAIA Manual, any processing notices issued to specific data subject categories, and any operator agreements concluded with third-party processors.

4. Lawful Basis for Processing

All processing of personal information by the AEC must have a lawful basis. POPIA provides the following lawful grounds for processing:

- The data subject has given consent to the processing.
- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party.
- Processing complies with a legal obligation imposed on the AEC.
- Processing protects a legitimate interest of the data subject.
- Processing is necessary for the pursuit of the AEC's legitimate organisational interests, provided these do not outweigh the privacy interests of the data subject.

Before collecting or processing any personal information, staff must identify and document the applicable lawful basis. Where no other lawful basis exists, consent must be obtained.

The processing of Special Personal Information (which includes race, health information, criminal records and information about minor children) is subject to additional restrictions and requires either explicit consent or reliance on a specific statutory ground. Given that the AEC's programme is specifically aimed at Black South African learners from the Alexandra community, race and residential information may be processed with the consent of the data subject, in terms of section

27(1)(a) of POPIA, to the extent strictly necessary to confirm eligibility, as is necessary to carry out the AEC's public benefit mission.

Further, where a data subject is under the age of 18, the personal information of that data subject may be processed with the consent of the data subject's parent or guardian, in terms of section 35(1)(a) of POPIA.

5. Consent

Where consent is the lawful basis for processing, the following requirements apply:

- Consent must be freely given, specific, informed and unambiguous.
- A separate consent must be obtained for each distinct purpose of processing.
- Consent may not be a condition of receiving services or benefits unless the processing is genuinely necessary for those services.
- For minor learners (under 18), consent must be obtained from a parent or competent guardian.
- Records of consent must be retained for the duration of the relationship with the data subject and for five years thereafter.

A data subject may withdraw consent at any time by providing written notice to the IO or DIO. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal. Upon receipt of a valid withdrawal notice, the AEC will stop processing unless another lawful basis applies or processing is necessary for the establishment, exercise or defence of a legal claim.

The IO or DIO is responsible for maintaining a consent register and for communicating the effects of any withdrawal to the relevant staff.

6. Purpose Limitation

Personal information collected by the AEC may only be used for the purpose for which it was collected and for no other incompatible purpose. In particular:

- Information collected for the administration of a bursary may not be used for unrelated fundraising or marketing purposes without separate consent.
- Donor information collected for the purpose of issuing tax receipts and programme reporting may not be sold or transferred to third-party fundraisers.
- Employee information collected for human resources purposes may not be used for purposes unrelated to the employment relationship.

If the AEC wishes to use personal information for a new purpose, it must either obtain consent or satisfy itself that the new purpose is compatible with the original purpose and that data subjects have been notified of the change.

Section 15(2) of POPIA sets out the factors a responsible party should consider in assessing whether further processing is compatible with the purpose for which it was collected. These factors are:

- (i) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
- (ii) the nature of the information concerned;
- (iii) the consequences of the intended further processing for the data subject;
- (iv) the manner in which the information has been collected; and
- (v) any contractual rights and obligations between the parties.

All staff must ensure that before collecting or processing personal information, there is a clearly documented and legitimate reason for the processing, and that data subjects are informed of that reason through a processing notice.

7. Accuracy

The AEC must ensure that all personal information it holds is accurate, complete and, where necessary, kept up to date. To meet this obligation, staff must:

- Take reasonable steps to ensure accuracy at the point of collection.
- Promptly update records when notified of a change by a data subject.
- Conduct periodic reviews of records (at least annually for active learner and donor records) to identify and correct inaccuracies.
- Delete or anonymise records where the information is no longer accurate and no legal basis for retention exists.

Data subjects have the right to request correction of inaccurate or outdated information. All such requests must be directed to the IO or DIO, who must respond within 30 days. The AEC will restrict the processing of such information for the period it takes for the IO or DIO to investigate and respond to such request.

8. Data Minimisation

The AEC may only collect and process personal information that is adequate, relevant and not excessive in relation to the purpose for which it is collected.

Before introducing new forms, systems or data collection processes, the responsible staff member must review the information being requested and remove any fields that are not strictly necessary for the stated purpose.

The AEC does not collect biometric data (fingerprints, voiceprints, retinal scans, etc.) other than photographs where these are required for identification or programme documentation purposes, and only with the data subject's knowledge and consent.

9. Transparency and Processing Notices

The AEC has a duty to deal with data subjects transparently. Before collecting personal information (or as soon as reasonably practicable thereafter), data subjects must be informed of:

- The identity and contact details of the AEC and the IO.
- The purpose for which the information is collected.
- Whether the supply of information is voluntary or mandatory, and the consequences of not providing it.
- Whether the information will be shared with third parties, and if so, who those parties are.
- The data subject's rights under POPIA.

The AEC maintains the following processing notices for different categories of data subjects:

- Learner and Bursary Applicant Processing Notice — issued at application stage and on enrolment.
- Parent/Guardian Processing Notice — issued with learner application forms and consent documents.
- Donor Processing Notice — included in donor agreements and on the AEC website.
- Employee Processing Notice — incorporated into employment contracts and the onboarding process.
- Contractor/Operator Processing Notice — included in operator agreements.

All forms and documents that collect personal information must reference the applicable processing notice or contain a brief privacy statement directing data subjects to the full notice available at www.alexeducation.org.za.

10. Security of Personal Information

The AEC is committed to protecting personal information against loss, damage, unauthorised access, destruction and unlawful processing. The following security measures are in place:

10.1 Technical Measures

- Anti-virus and endpoint security software on all staff computers and shared systems, monitored and maintained by the AEC's IT service provider.
- Strong password standards enforced on all devices and systems.
- Secure cloud-based and on-site storage with password-controlled access and regular backups.
- Role-based access controls — staff may only access personal information necessary for their duties.
- Electronic transmission of personal information via encrypted channels where feasible.

10.2 Organisational Measures

- All staff are made aware of their obligations under POPIA and this Policy during induction and through annual refresher training.
- Paper-based records containing personal information must be stored in locked cabinets when not in use and may not be left unattended on desks or printers.

- Personal information must not be discussed in public spaces or shared with unauthorised individuals.
- Devices must be locked when left unattended.
- On termination of employment or change of role, access rights must be revoked immediately by the IO in conjunction with the IT service provider.
- Written operator agreements are in place with all third parties who process personal information on the AEC's behalf.

10.3 Special Personal Information

Access to Special Personal Information (including health information about learners) requires specific authorisation by the IO and is restricted to staff with a documented need to access such information for programme purposes.

11. Records Management

All records containing personal information must be created, stored and managed in accordance with the following requirements:

- Records must be clearly named and classified according to their sensitivity (Public, Internal, Confidential or Restricted).
- Records must be stored in designated secure folders or filing systems.
- Records must be accessible only to authorised personnel on a need-to-know basis.
- Paper records must be stored in locked cabinets. Electronic records must be stored on the AEC's secure server or approved cloud storage managed by the IT service provider.
- Confidential records may not be stored on personal devices, USB drives or removable media without explicit authorisation from the IO, and must be encrypted if so stored.
- Records may not be removed from AEC premises without authorisation and must be returned or securely destroyed after use.

The IO maintains a records management register that documents the categories of records held, their format, location, access controls, retention period and disposal method.

12. Retention and Disposal

Personal information may not be retained longer than is necessary for the purpose for which it was collected, unless a longer period is required by law; justified by a legitimate organisational interest relating to the AEC's functions or activities; is required by contract between the parties; or where consent has been obtained.

The AEC's standard retention periods are set out in the PAIA Manual and summarised below:

Category	Retention Period	Notes
Learner / bursary records	7 years post-programme exit	Includes academic records, correspondence, bursary agreements
Employee records	As required by applicable employment legislation	Minimum 3–5 years post-termination for most records
Donor records	7 years post-donation	Section 18A tax compliance; FICA requirements
Financial records	7 years	As required by SARS and NPO Act
Annual reports and audited financial statements	Indefinite	Publicly available; historical record
Founding documents / Constitution	Indefinite	NPO and PBO compliance
Contractor records	Duration of contract + 5 years	As required by applicable legislation and contracts

When the retention period has expired, records must be securely destroyed. Paper records must be shredded. Electronic records must be permanently deleted using a method that prevents recovery. Any disposal must be authorised by the IO and recorded in the records management register.

Records may not be destroyed if they are subject to a pending legal claim, regulatory inquiry or PAIA request.

13. Operators and Third-Party Processors

Where the AEC engages a third party to process personal information on its behalf (an Operator), the AEC must ensure that:

- A written operator agreement is in place before any personal information is shared with the Operator.
- The agreement requires the Operator to process personal information only as instructed by the AEC, to maintain adequate security measures and to notify the AEC immediately of any security incident or breach.
- The Operator may not engage sub-operators without prior written consent from the AEC.
- The AEC retains the right to audit the Operator's compliance with the agreement.

Current operators include (but are not limited to):

- The AEC's IT service provider — responsible for IT infrastructure, cloud storage, email platforms, endpoint security and system maintenance.
- Payroll and accounting service providers.
- Any cloud-based software platforms used for learner management, donor management or HR functions.

The IO must maintain an operator register and ensure all agreements are current. Any new engagement with a third-party processor must be approved by the IO before commencement.

14. Sharing Personal Information with Third Parties

The AEC does not sell, rent or trade personal information to or with third parties. Personal information may only be shared with a third party where:

- There is a legitimate organisational basis for doing so and the third party has agreed (through a signed agreement) to keep the information confidential;
- The data subject has consented to the sharing; or
- The sharing is required by law (e.g. reporting to SARS, the Department of Labour or another regulatory authority).

Specific examples of permitted sharing include:

- Sharing academic records with partner schools for the purposes of administering the bursary programme.
- Sharing contact and payment information with transport and uniform suppliers to the extent necessary to fulfil programme obligations.
- Sharing anonymised or aggregated impact data with donors for reporting purposes.
- Sharing information with SARS for the purposes of issuing Section 18A tax receipts.

When sending personal information by email, it must be placed in a password-protected or encrypted attachment rather than the body of the email. All such emails must be marked Confidential.

15. Cross-Border Transfers of Personal Information

Personal information may not be transferred to a recipient in a country outside of South Africa unless adequate safeguards are in place; the recipient is subject to law, binding corporate rules, or a binding agreement that imposes obligations equivalent to POPIA; or the data subject has expressly consented to the transfer, having been informed of any associated risks.

Cloud services used by the AEC may involve servers located outside South Africa. The IO must confirm annually whether any such transfers occur and document the legal basis for such transfers. Where transfers occur, they must be disclosed in the AEC's PAIA Manual (see section 5.7.7 of the May 2026 edition).

16. Direct Marketing and Communications

The AEC communicates with various stakeholders including donors, alumni, partner schools and the general public. All communications involving personal information must comply with POPIA.

- Unsolicited direct electronic marketing (email, SMS, WhatsApp) to individuals who are not existing contacts of the AEC is prohibited unless the individual has opted in.

- All marketing and newsletter communications must include a clear, free opt-out mechanism.
- When a data subject opts out, their details must be removed from the relevant mailing list within a reasonable period (and no later than 14 days) and must not be contacted again for that purpose.
- For donors and supporters who are existing contacts, the AEC may send programme updates and impact reports based on its legitimate organisational interests, provided an opt-out is always included.

All opt-in and opt-out records must be maintained by the IO or their delegate.

17. Reporting Personal Information Breaches

A personal information breach is any event that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information held by the AEC.

All staff have a duty to report any suspected or known breach immediately to the IO. The IO will investigate and, where the breach meets the threshold under section 22 of POPIA, will notify the Information Regulator and the affected data subjects as soon as reasonably possible.

A breach notification must include:

- A description of the breach, including its likely cause and the categories and approximate number of data subjects and records affected.
- The likely consequences of the breach.
- The measures taken or proposed to address the breach and to mitigate its adverse effects.
- A recommendation to the affected data subjects of measures to be taken to mitigate any possible adverse effects of the breach.
- Where possible, the identity of the unauthorised person who may have accessed or acquired the records.

Staff must not communicate with external parties, regulators or media about a breach without the IO's authorisation. All breach records must be retained and the incident documented using Schedule B of this Policy.

The AEC will cooperate fully with the Information Regulator in any investigation arising from a breach.

18. Data Subject Rights and Requests

POPIA confers the following rights on data subjects in respect of their personal information held by the AEC:

- The right to be notified when personal information about them is being collected.
- The right to confirm whether the AEC holds personal information about them (free of charge).
- The right to access their personal information (subject to PAIA procedures and fees).
- The right to request correction or deletion of inaccurate or outdated personal information.

- The right to object to processing, including for direct marketing purposes.
- The right to withdraw consent at any time.
- The right to be notified of a personal information breach affecting them.
- The right to lodge a complaint with the Information Regulator.

All requests to exercise these rights must be directed to the IO or DIO:

- Email: director@alexeducation.org.za | bron@alexeducation.org.za
- Address: 1 Knox Street, Waverley, Johannesburg (PO Box 1938, Highlands North, 2037)

The IO or DIO will acknowledge receipt of any request within five business days and respond substantively within 30 days. Requests for access to records must be made on the Form C prescribed in terms of PAIA (available as Schedule B to the AEC's PAIA Manual or at www.alexeducation.org.za).

19. The Right to Complain

Any data subject who is dissatisfied with the manner in which the AEC has processed their personal information may submit a complaint to the IO in writing. The IO will acknowledge the complaint within five business days and attempt to resolve it within 30 days.

If the matter is not resolved to the data subject's satisfaction, the data subject may refer the complaint to the Information Regulator at:

- The Information Regulator (South Africa), JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
- Email: infoereg@justice.gov.za / complaints.IR@justice.gov.za
- Tel: +27 (0)10 023-5200

20. Governance

The Information Officer (currently the Executive Director, Paul Kevan Channon) is responsible for:

- Overall oversight of POPIA compliance within the AEC.
- Developing, implementing and updating this Policy and any associated processing notices and procedures.
- Responding to data subject rights requests, complaints and regulatory enquiries.
- Ensuring that operator agreements are concluded with all third-party processors.
- Overseeing the response to any personal information breach.
- Ensuring that the PAIA Manual and this Policy are reviewed at least annually.

The Deputy Information Officer (Bronwynne Viljoen) assists the IO with these responsibilities and acts in the IO's absence.

Council members are responsible for ensuring that this Policy is resourced, reviewed and complied with as part of the AEC's governance framework.

All staff and volunteers are responsible for complying with this Policy in their daily work and for immediately reporting any suspected breach or non-compliance to the IO.

21. Training and Awareness

The IO will ensure that:

- All new staff and volunteers receive POPIA awareness training as part of their induction.
- All staff complete refresher training at least annually.
- This Policy is accessible to all staff at all times (on the AEC's internal systems and website).
- Any significant changes to POPIA or to this Policy are communicated to staff promptly.

The IO may engage external advisers or the Information Regulator's resources to support training and compliance efforts.

22. Non-Compliance

Compliance with this Policy is mandatory for all staff, volunteers and contractors. Any breach of this Policy will be treated seriously and may result in:

- Disciplinary action, up to and including dismissal, in the case of employees.
- Termination of a volunteer or contractor arrangement.
- Referral to the Information Regulator where the breach constitutes an offence under POPIA.

Non-compliance with POPIA may expose the AEC to enforcement action by the Information Regulator, including fines of up to R10 million and potential imprisonment of responsible individuals. It also risks reputational harm to the AEC and undermines the trust of the learners, donors and communities it serves.

23. Version and Amendments

This Policy is effective from June 2026 and supersedes any prior POPIA policy or data protection guidance issued by the AEC.

The AEC reserves the right to amend this Policy at any time to reflect changes in the law, organisational practices or guidance from the Information Regulator. The most current version will be made available on the AEC's website at www.alexeducation.org.za and at the AEC's offices. Staff will be notified of any material changes.

Next scheduled review: March 2027.

Schedule A — Data Subject Categories and Processing Purposes

The following table summarises the categories of data subjects whose personal information is processed by the AEC, the categories of information held, the purposes of processing and the likely recipients of that information.

Data Subject	Key Personal Information	Purpose of Processing	Likely Recipients
Bursary Applicants	Personal details, ID, academic records, household income, residence information	Eligibility assessment; selection process; applicant notification	IO; programme staff; selection panel
Current Bursars (High School)	Personal details, ID, academic records, bursary agreement, school fees, transport and uniform details, laptop allocation, health info (welfare)	Bursary administration; academic monitoring; welfare; donor reporting (anonymised)	IO; programme staff; partner schools; transport/service providers; donors (anonymised)
Saturday School Learners (Gr 5–7)	Personal details, school attended, academic performance, parent/guardian contact details	Programme administration; academic monitoring; parent communication	IO; programme staff; partner schools
Parents/Guardians	Contact details, household income (bursary applicants), consent records	Consent; programme communication; welfare of minor learners	IO; programme staff
Donors (Individuals and Corporates)	Contact details, company registration (corporates), donation amounts and dates, Section 18A tax info	Donor relationship management; Section 18A receipts; FICA compliance; programme reporting	IO; finance; SARS
Employees	HR records, employment contract, payroll, tax, leave, disciplinary records	Employment administration; statutory compliance; payroll	IO; finance; line management; statutory bodies
Contractors / Service Providers	Company registration, contact and banking details, services rendered	Service delivery; contract management; payment	IO; finance

Schedule B — Personal Information Breach Report Form

To be completed by the staff member who discovers or suspects a personal information breach and submitted immediately to the Information Officer.

Person Reporting (may be anonymous)	
Date and Time Incident Discovered	
Date and Time Reported to IO	
Programme/Department	
Type of Personal Information Affected	
Approximate Number of Data Subjects Affected	
Description of the Incident	
Likely Cause of Breach	
Likely Consequences	
Immediate Steps Taken	
Further Action Proposed	

Signature: _____ Date: _____

IO Acknowledgement: _____ Date: _____