



YALPAE

**YOUNG AFRICAN LEADERS
PIONEERS AND ENTREPRENEURS**

Africa's Light, paying forward to the future

**DATA & INTELLECTUAL
PROPERTY
ANNEX H
MARCH 2026**



YALPAE Policy

LEGAL STATEMENT

This document constitutes an official governance instrument of Young African Leaders, Pioneers and Entrepreneurs (YALPAE), a registered Non-Profit Company operating in accordance with the laws of the Republic of South Africa.

This document is classified under the YALPAE Policy Class, within which all policies, frameworks, declarations, and operational instruments are maintained as part of an integrated governance system. This document forms part of YALPAE's internal governance framework and shall be read together with the YALPAE Constitution, By-Laws, Mandate, and all applicable Annexes and policies.

This document applies to all persons acting under the authority, representation, or auspices of YALPAE, including members, directors, officers, volunteers, partners, and affiliated participants.

AUTHORITY CLAUSE

This document is issued under the authority of the YALPAE Board of Directors in accordance with the YALPAE Constitution and By-Laws.

Its provisions derive their authority from, and must be interpreted consistently with:

- The YALPAE Constitution
- The YALPAE By-Laws
- The YALPAE Mandate
- All applicable Annexes, including the Code of Conduct and Safeguarding Framework

In the event of any inconsistency:

- The Constitution shall prevail
- Safeguarding provisions shall take precedence in all safeguarding-related matters
- This document shall govern operational implementation within its defined scope

COPYRIGHT AND OWNERSHIP

This document and all associated content are the intellectual property of Young African Leaders, Pioneers and Entrepreneurs (YALPAE).

No part of this document may be reproduced, distributed, modified, or used for commercial or organisational purposes without prior written consent from YALPAE, except where required for internal use in accordance with YALPAE's governance and operational activities.

Unauthorised use, reproduction, or misrepresentation of this document may result in disciplinary action or legal consequences in accordance with applicable laws and YALPAE policies.



DATA & INTELLECTUAL PROPERTY POLICY

Content Page

Content	Page No.
PREAMBLE	1
PURPOSE	1
LEGAL FRAMEWORK & CONSTITUTIONAL AUTHORITY	2
SCOPE OF APPLICATION	3
DEFINITIONS	4
DATA PROTECTION PRINCIPLES	5
LAWFUL BASIS FOR PROCESSING	5
CATEGORIES OF DATA COLLECTED	6-7
GENERAL PERSONAL INFORMATION	6
SENSITIVE OR HIGHER-RISK INFORMATION	6
SPECIFIC PERSONAL INFORMATION	6
RECORDING NOTICE	7
CHILDREN'S INFORMATION	7
PURPOSE OF DATA USE	7
INFORMATION QUALITY & DATA MINIMISATION	8
DATA STORAGE, ACCESS & SECURITY	8
DATA SHARING, THIRD PARTIES & CROSS-BORDER TRANSFERS	9
DATA BREACH RESPONSE	9
INFORMATION OFFICER	10
INTELLECTUAL PROPERTY OWNERSHIP	11
DATA RETENTION, RESTRICTION & DELETION	12
DATA SUBJECT RIGHTS	13
ACCOUNTABILITY, BREACH & ENFORCEMENT	14
REVIEW & AMENDMENTS	15

ANNEX H: DATA PROTECTION & INTELLECTUAL PROPERTY POLICY

PREAMBLE

YALPAE is a youth-led, Pan-African non-profit organisation registered in the Republic of South Africa. In conducting its work across national and continental contexts, YALPAE processes personal information, stores institutional records, and creates or uses intellectual property in the ordinary course of its governance, programmes, partnerships, and public communications.

This Policy establishes how YALPAE meets its legal and ethical obligations in relation to data protection, privacy, and intellectual property. It is adopted pursuant to the YALPAE Constitution and By-Laws and must be read together with all applicable governance instruments and South African law.

Compliance with this Policy is a condition of membership, leadership, participation, appointment, volunteering, employment, and partnership.

1. PURPOSE

This Policy sets out how YALPAE:

- collects, processes, stores, shares, protects, archives, and deletes personal and organisational information;
- respects the privacy, dignity, and rights of individuals, with heightened protection for children and vulnerable persons;
- manages ownership, use, protection, licensing, and enforcement of intellectual property and brand assets;
- establishes accountability, procedures, and consequences for non-compliance.

This Policy exists to enable YALPAE's work responsibly. It is intended to strengthen trust, institutional discipline, and lawful processing rather than restrict legitimate participation.

2. LEGAL FRAMEWORK & CONSTITUTIONAL AUTHORITY

2.1 Constitutional Authority

This Policy is adopted pursuant to the YALPAE Constitution, including its provisions on intellectual property, data privacy, data security, safeguarding, and institutional accountability.

2.2 Primary Legislation

This Policy must be interpreted consistently with:

- **POPIA** as the primary data protection statute governing the lawful processing of personal information;
- **PAIA** in respect of access to records held by private bodies and the maintenance of a PAIA manual where required;
- **ECTA** in relation to electronic communications and records;
- the **Children's Act** in relation to the best interests of the child;
- the **Copyright Act** and **Trade Marks Act** in relation to ownership and protection of YALPAE's content and brand;
- any other applicable law in any jurisdiction where YALPAE operates.

2.3 Relationship to YALPAE Governance Instruments

This Policy must be read together with:

- the YALPAE Constitution;
- the YALPAE By-Laws;
- the Child Protection & Safeguarding Framework;
- the Code of Conduct & Ethics;
- the Leadership Ethics Addendum;
- the Partnership & Sponsorship Governance instrument.

Where any conflict arises between this Policy and the Constitution, the Constitution prevails. Where any conflict arises between this Policy and safeguarding obligations, safeguarding obligations prevail to the extent necessary to protect a child or vulnerable person.

3. SCOPE OF APPLICATION

This Policy applies to:

- all personal information collected, received, processed, or stored by YALPAE, regardless of format;
- all organisational, governance, operational, financial, programmatic, and communications records;
- all intellectual property created, commissioned, used, or shared under YALPAE's name or authority;
- all platforms, systems, devices, repositories, forms, archives, and tools used by YALPAE, whether digital or physical;
- all persons acting under YALPAE's name, authority, or auspices, including Board members, Executive Committee members, officers, staff, members, volunteers, chapter representatives, partners, operators, sponsors, contractors, and service providers.

Compliance with this Policy is a non-negotiable condition of membership, leadership, participation, employment, appointment, volunteering, and partnership.

4. DEFINITIONS

For the purposes of this Policy, unless the context otherwise requires:

Term	Definition
Personal Information	Information relating to an identifiable, living natural person and, where applicable, an identifiable juristic person.
Special Personal Information	Personal information regulated under POPIA Part B, including categories such as religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and criminal behaviour, subject to sections 26 to 33.
Sensitive Information	A stricter internal YALPAE handling category that may include ID numbers, passport details, education records, images, recordings, safeguarding records, and other higher-risk information, whether or not it falls within POPIA's special-personal-information category.
Processing	Any operation involving personal information, including collection, receipt, recording, organisation, storage, use, sharing, restriction, deletion, destruction, or de-identification.
Responsible Party	YALPAE, as the body that determines the purpose of and means for processing personal information.
Operator	A third party that processes personal information for YALPAE in terms of a mandate or service arrangement.
Information Officer	The designated officer responsible for oversight of POPIA and PAIA compliance within YALPAE.
Data Subject	The person or entity to whom personal information relates.
Child / Junior Member	Any person under the age of eighteen (18) years.
Safeguarding Record	Any record relating to a safeguarding concern, allegation, protective action, investigation, or outcome involving a child or vulnerable person.
Intellectual Property (IP)	YALPAE's original works, branding, logos, trade marks, documents, frameworks, methodologies, databases, content, designs, media, and materials created by, for, or on behalf of YALPAE.
Data Breach / Security Compromise	Unauthorised access to, acquisition of, destruction of, alteration of, or interference with personal information held by YALPAE.

POPIA's statutory definitions prevail where the Act expressly defines a term. The conditions for lawful processing, the prohibition on special personal information, the prohibition on processing children's information except where authorised, the Information Officer's role, and cross-border transfer rules are set by POPIA sections 4, 26, 34 to 35, 55, and 72. _____

5. DATA PROTECTION PRINCIPLES

YALPAE processes personal information in accordance with the eight conditions for lawful processing established by POPIA Chapter 3. These include accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. _____

Accordingly, all processing under this Policy must comply with the following principles:

- **Accountability** — YALPAE, as the Responsible Party, remains accountable for compliance with POPIA and this Policy.
- **Processing Limitation** — Personal information may be processed only where a lawful basis exists and only in a manner that is adequate, relevant, and not excessive.
- **Purpose Specification** — Personal information must be collected for a specific, explicitly defined, and lawful purpose.
- **Further Processing Limitation** — Further processing must be compatible with the purpose for which the information was collected.
- **Information Quality** — Reasonable steps must be taken to ensure information is complete, accurate, not misleading, and updated where necessary.
- **Openness** — YALPAE must maintain documentation of processing and notify data subjects appropriately when collecting their information.
- **Security Safeguards** — Reasonable technical and organisational measures must be implemented to protect information.
- **Data Subject Participation** — Data subjects are entitled to access, correct, object to certain processing, and exercise other rights provided by law.

No personal information may be processed in a manner that is unlawful, exploitative, deceptive, excessive, or inconsistent with YALPAE's mission and governance obligations.

6. LAWFUL BASIS FOR PROCESSING

YALPAE processes personal information only where a lawful basis exists under section 11 of POPIA. These bases include consent, contractual necessity, legal obligation, protection of a legitimate interest of the data subject, performance of a public-law duty by a public body where applicable, and legitimate interests pursued by the responsible party or an authorised third party. POPIA also provides that a data subject or competent person may withdraw consent and may object to certain forms of processing. _____

YALPAE will generally rely on one or more of the following grounds:

- **Consent** — where the data subject, or a competent person in the case of a child, has given voluntary, specific, and informed consent;
- **Contractual necessity** — where processing is necessary to conclude or perform a membership, volunteering, service, employment, or participation arrangement;

- **Legal obligation** — where processing is required for compliance with law, governance, safeguarding, or regulatory obligations;
- **Legitimate interests of the data subject** — where processing is necessary to protect the data subject's lawful interests;
- **Legitimate interests of YALPAE or an authorised third party** — where processing is necessary for governance, administration, programme delivery, communication, reporting, or institutional continuity, and does not unlawfully override the data subject's rights.

YALPAE shall not process personal information on vague, convenience-based, or undefined grounds.

7. CATEGORIES OF DATA COLLECTED

7.1 General Personal Information

YALPAE may collect general personal information including:

- full names and surnames;
- contact details;
- date of birth or age category where necessary;
- membership category and participation records;
- chapter affiliation and role information;
- communications and attendance records.

7.2 Sensitive or Higher-Risk Information

YALPAE shall not collect higher-risk information by default. Where necessary, justified, and lawful, it may process:

- ID or passport numbers;
- education and qualification records;
- health, wellness, disability, access, or accommodation information;
- photographs, audio, and video recordings;
- criminal-background information where lawful and safeguarding-justified;
- safeguarding, disciplinary, or investigation records.

7.3 Special Personal Information

Where information constitutes **Special Personal Information** under POPIA, YALPAE shall process it only where a lawful exemption, authorisation, or explicit consent requirement is satisfied, and only for a clearly defined purpose under sections 26 to 33. _____

7.4 Recording Notice

Where meetings, sessions, events, or programmes are recorded, YALPAE shall provide a clear prior notice and disclaimer wherever reasonably practicable.

8. CHILDREN'S INFORMATION

The processing of personal information relating to children is subject to heightened protection. POPIA prohibits the processing of children's personal information unless one of the section 35 conditions applies or the Regulator has granted authorisation. The Act separately prohibits special personal information of children unless the relevant authorisation conditions are met. _____

Accordingly, YALPAE shall:

- collect only the minimum information necessary for a child's participation, safety, or lawful administration;
- obtain parental or guardian consent where required by law, safeguarding policy, or programme design;
- use children's information strictly for approved organisational, safeguarding, participation, or legal purposes;
- apply additional access restrictions and confidentiality controls to children's information and safeguarding records;
- never use children's information for profiling, non-essential marketing, or unnecessary publication.

The best interests of the child shall be a primary consideration in any decision involving the processing, disclosure, restriction, or retention of a child's personal information.

9. PURPOSE OF DATA USE

YALPAE processes information only for legitimate organisational purposes, including:

- programme delivery and participation;
- member communication and coordination;
- governance, compliance, and statutory reporting;
- operation of YALPAE's website and digital platforms;
- monitoring, evaluation, learning, and institutional reporting;
- safeguarding, disciplinary, and dispute-resolution processes;
- fundraising and partnership administration where lawful and appropriate.

Personal information shall never be used for personal gain, unrelated commercial exploitation, harassment, or purposes incompatible with the purpose for which it was collected.

10. INFORMATION QUALITY & DATA MINIMISATION

YALPAE shall take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated where necessary. Personal information may be processed only if, having regard to the purpose for which it is processed, it is adequate, relevant, and not excessive. POPIA anchors these requirements in sections 10 and 16. [_____](#)

Members, participants, and other data subjects are expected to provide accurate information and to notify YALPAE where material updates are necessary.

11. DATA STORAGE, ACCESS & SECURITY

11.1 Storage Systems

YALPAE may store information through:

- secure cloud-based platforms;
- approved organisational databases, forms, and repositories;
- physical files and registers maintained in secured environments;
- structured archival and backup systems.

11.2 Access Control

Access to information is role-based and limited to what is necessary for each function.

Role	Access Level
Information Officer	Primary privacy oversight and compliance coordination
Chairperson, Vice-Chairperson, Secretary, Treasurer	Governance, operational, and membership records necessary for their functions
Portfolio Directors and Committee Leads	Data directly relevant to their portfolio or committee function
Chapter Leaders	Localised member and participant data within their own chapter only
Partners and Sponsors	No default access to personal member data
Operators / Service Providers	Access only in terms of a written mandate and only for the approved purpose

11.3 Security Safeguards

YALPAE shall implement reasonable technical and organisational measures to protect personal information against loss, damage, unauthorised access, unlawful processing, or compromise, consistent with POPIA sections 19 to 22. These may include role-based access controls, restricted permissions, confidentiality obligations, secure storage, transmission safeguards, and breach-response procedures. Operators must be bound by written arrangements and must notify YALPAE where unauthorised access is reasonably suspected.

12. DATA SHARING, THIRD PARTIES & CROSS-BORDER TRANSFERS

YALPAE shares personal information only where such sharing is lawful, necessary, proportionate, and authorised. Sharing may occur with the data subject's consent, where required for programme delivery, where required by law, or where necessary for safeguarding, governance, or lawful reporting. Partner or sponsor access to personal member data is prohibited by default and requires a documented lawful basis plus appropriate safeguards. These rules sit within POPIA's openness, security, and transborder-flow framework, including sections 17 to 22 and section 72.

12.1 Permitted Sharing

Information may be disclosed where:

- the data subject has consented;
- disclosure is necessary for programme delivery or administration;
- disclosure is required by law, court order, or regulatory duty;
- disclosure is necessary for safeguarding, child protection, or protection of vital interests;
- disclosure is required for audit, compliance, or governance reporting.

12.2 Third-Party Operators

Where a third party processes personal information on YALPAE's behalf, that party must act only under a written operator agreement and must implement appropriate safeguards.

12.3 Cross-Border Transfers

YALPAE may transfer personal information outside South Africa only where permitted by section 72 of POPIA, including where the recipient is subject to substantially similar protections, the data subject has consented, the transfer is contractually necessary, or another lawful basis applies.

Higher-risk transfers involving children's information, safeguarding records, or special personal information require additional caution and approval.

13. DATA BREACH RESPONSE

Where there are reasonable grounds to believe personal information has been accessed or acquired by an unauthorised person, POPIA requires the responsible party to notify the Regulator and, subject to the Act, the affected data subject. YALPAE will also take immediate containment and corrective measures. _____

In the event of a security compromise, YALPAE shall:

- contain the breach and secure affected systems;
- assess the nature, scope, and likely consequences of the breach;
- notify the Information Regulator where required;
- notify affected data subjects where required and where a reasonable risk of harm exists;

- document the breach and the response;
- implement remedial and preventative measures.

Where a breach involves a child or a safeguarding-related record, the Safeguarding Focal Person and the Director of Youth Wellness & Protection must be notified immediately, and the safeguarding framework applies concurrently.

14. INFORMATION OFFICER

In accordance with POPIA section 55, the Information Officer's responsibilities include encouraging compliance with the conditions for lawful processing, dealing with requests made under the Act, and working with the Regulator. The Information Regulator also requires Information Officers and Deputy Information Officers to be registered before acting in that role. PAIA separately requires private bodies to compile a manual under section 51. _____

The Board shall therefore appoint or designate an Information Officer responsible for:

- overseeing YALPAE's compliance with POPIA and this Policy;
- handling access, correction, deletion, and objection requests;
- coordinating breach response and reporting;
- maintaining or coordinating the organisation's PAIA manual where required;
- serving as the primary internal contact for privacy matters;
- liaising with the Information Regulator where necessary. **Information Regulator of South Africa**

General enquiries: **010 023 5200**

Toll-free: **0800 017 160**

Email: enquiries@inforegulator.org.za

Website: www.inforegulator.org.za ([Inforegulator](http://inforegulator.org.za))

15. INTELLECTUAL PROPERTY OWNERSHIP

Unless otherwise agreed in writing, all intellectual property created, developed, commissioned, or acquired by YALPAE, or created by any member, volunteer, officer, staff member, or contractor in the course of their YALPAE duties, vests in YALPAE. This includes YALPAE's name, logo, visual identity, policies, governance frameworks, reports, publications, training materials, programme content, databases, websites, and organisational systems.

15.1 YALPAE-Owned IP

This includes, without limitation:

- the YALPAE name, logo, and associated brand assets;
- policies, constitutions, by-laws, annexes, and governance instruments;
- reports, manuals, templates, concept notes, toolkits, and training materials;
- campaign materials, publications, and media outputs;
- websites, databases, and systems created for YALPAE.

15.2 Contributor Materials

By contributing to YALPAE work in a YALPAE capacity, contributors grant YALPAE a royalty-free, worldwide licence to use, reproduce, adapt, publish, distribute, and archive those contributions for YALPAE purposes. Where needed to avoid legal uncertainty, YALPAE may require assignment of relevant rights.

15.3 Pre-Existing and Third-Party IP

Pre-existing intellectual property brought into a YALPAE project remains the property of the original owner unless expressly assigned in writing. Third-party content must not be used without appropriate licence, permission, or lawful basis.

15.4 Brand Protection

No one may use YALPAE's name, logo, branding, or official materials publicly in a way that implies endorsement, institutional authority, or partnership without authorisation.

16. DATA RETENTION, RESTRICTION & DELETION

POPIA section 14 requires that personal information not be retained for longer than reasonably necessary, subject to legal, contractual, safeguarding, archival, or proof-related grounds for continued retention. It also requires destruction, deletion, or de-identification when retention is no longer authorised, and restriction in certain cases. _____

YALPAE shall apply the following retention framework:

Category	Retention Period	Notes
Active member records	Duration of active membership	Maintained while membership is active and for legitimate administrative continuity
Former member records	Up to 6 months after termination or withdrawal	Unless retention is justified by law, safeguarding, dispute, finance, or governance needs
Junior member participation records	Duration of programme participation plus up to 12 months	Subject to safeguarding, consent, and programme-specific needs
Safeguarding records	As long as reasonably necessary for child protection, legal accountability, or safeguarding obligations	May be retained for an extended or indefinite period where lawful and necessary
Disciplinary and investigation records	Minimum 5 years from closure	Longer if appeals, disputes, or legal proceedings continue
Board, governance, and constitutional records	Permanent archive	Institutional memory and governance continuity
Financial and audit records	Minimum 5 years or longer if required by law	Includes agreements, approvals, and supporting records
Partnership and sponsorship agreements	Duration of agreement plus 5 years	Longer if IP, dispute, or compliance issues remain live
Recruitment, volunteer, and appointment records	Up to 2 years after conclusion	Unless retained longer for legal or governance reasons
Website and digital-system logs	As operationally necessary and proportionate	Subject to security, troubleshooting, and lawful-use requirements

Upon expiry of the applicable retention period, personal information must be deleted, destroyed, or de-identified in a secure manner that prevents intelligible reconstruction, unless lawful grounds for continued retention remain.

17. DATA SUBJECT RIGHTS

POPIA gives data subjects enforceable participation rights, including the right to be notified of collection and unauthorised access, to request access, to seek correction or deletion, to object to certain processing, to complain to the Regulator, and to institute civil proceedings. The five core rights below should be read together with POPIA sections 5, 11(2)(b), 11(3), 23, 24, and 74.

17.1 Right of Access

A data subject may request confirmation of whether YALPAE holds personal information about them and may request access to that information, subject to proof of identity and lawful limitations. **(POPIA s23)**

17.2 Right to Correction, Destruction or Deletion

A data subject may request correction or deletion of information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, unlawfully obtained, or no longer lawfully retainable. **(POPIA s24)**

17.3 Right to Object

A data subject may object, on reasonable grounds relating to their particular situation, to processing based on legitimate-interest grounds, and may object to direct marketing as permitted by law. **(POPIA s11(3))**

17.4 Right to Withdraw Consent

Where processing is based on consent, the data subject or competent person may withdraw that consent at any time, without affecting processing already lawfully undertaken before withdrawal. **(POPIA s11(2)(b))**

17.5 Right to Lodge a Complaint

A data subject may submit a complaint to the Information Regulator where they believe their personal information has been processed in a manner that interferes with their rights. **(POPIA s74)**

Requests must be directed to the Information Officer and will be handled within a reasonable time and in accordance with applicable law. Nothing in this section requires YALPAE to disclose information where disclosure would be unlawful, would compromise safeguarding duties, or would otherwise fall within a lawful ground of refusal.

18. ACCOUNTABILITY, BREACH & ENFORCEMENT

YALPAE, as the Responsible Party, remains accountable for ensuring compliance with this Policy and with POPIA's conditions for lawful processing. POPIA's accountability condition, security-safeguards regime, and breach-notification rule sit principally in sections 8 and 19 to 22. ([Justice](#))

Oversight and enforcement responsibility is allocated as follows:

- **Information Officer** — primary oversight of POPIA and PAIA compliance, breach response, and data-subject requests;
- **Board of Directors** — ultimate organisational accountability and authority to direct corrective, disciplinary, or legal action;
- **Directors, officers, committee leads, and chapter leaders** — accountability for compliance within their functions and delegated areas.

Breaches of this Policy may result in:

- corrective guidance or remedial training;
- restriction or removal of access to systems or records;
- takedown or withdrawal of unauthorised material;
- suspension from duties, participation, or leadership;
- termination of role, contract, membership, or engagement;
- referral to the Board, Information Officer, Ethics Officer, Membership Committee, or Safeguarding Focal Person;
- referral to regulators or competent authorities where required.

Responsible Party: For purposes of POPIA, YALPAE acts as the **Responsible Party** in respect of all personal information processed under its authority and remains accountable for compliance, even where processing is delegated to Operators, contractors, chapters, platforms, or service providers.

19. REVIEW & AMENDMENT

This Policy shall be reviewed at least every two (2) years, or sooner where required by:

- changes in law or regulator guidance;
- material operational or digital-system changes;
- safeguarding developments;
- identified compliance gaps or organisational risk;
- Board resolution.

Amendments to this Policy require approval by the Board of Directors and must remain consistent with the YALPAE Constitution and applicable law.

POPIA Supremacy: Where any provision of this Policy conflicts with applicable data protection law, including the **Protection of Personal Information Act 4 of 2013 (POPIA)**, the **higher legal standard shall prevail**. POPIA itself also provides that where another law imposes more extensive lawful-processing conditions, the more extensive conditions prevail. ([Justice](#))

