

PNEUMA AFRICAN FOUNDATION

PRIVACY POLICY

Document Number: PAF-GOV-001

Version: 1.0

Effective Date: 30 July 2026

Approval Authority: Board of Directors, Pneuma African Foundation

Review Cycle: Every Two (2) Years or Earlier if Required by Law

Document Classification: Public Governance Document

Table of Contents

1. Preamble
 2. Purpose of this Privacy Policy
 3. About Pneuma African Foundation
 4. Our Commitment to Privacy
 5. Scope and Application
 6. Definitions
 7. Privacy Principles
 8. Lawful Basis for Processing Personal Information
 9. Contact Information
 10. Policy Interpretation
-

1. PREAMBLE

Pneuma African Foundation ("**the Foundation**", "**PAF**", "**we**", "**our**", or "**us**") recognizes that privacy is a fundamental human right and an essential component of dignity, trust, accountability, and responsible stewardship. As an international civil society organization committed to transforming vulnerable communities through sustainable development and humanitarian action, we understand that individuals who engage with our work entrust us with their personal information in confidence.

This Privacy Policy establishes the principles and standards governing the collection, use, storage, disclosure, transfer, protection, and disposal of personal information processed by Pneuma African Foundation through its website, digital platforms, fundraising activities, humanitarian programmes, volunteer services, partnerships, and other operational activities.

Our commitment extends beyond legal compliance. We believe that responsible management of personal information reflects our values of integrity, transparency, accountability, respect for human dignity, and ethical service. Every donor, volunteer, beneficiary, partner,

employee, consultant, contractor, supporter, and visitor has the right to expect that their personal information will be handled lawfully, fairly, securely, and with respect.

This Privacy Policy forms part of the Foundation's broader governance framework and should be read together with other applicable organisational policies, including our Terms and Conditions, Donation Policy, Safeguarding Policy, Child Protection Policy, Data Protection Policy, Code of Conduct, and other governance documents adopted by the Foundation.

2. PURPOSE OF THIS PRIVACY POLICY

The purpose of this Privacy Policy is to:

- explain what personal information Pneuma African Foundation collects;
- describe how and why such information is collected;
- outline how personal information is used, stored, protected, retained, and, where necessary, shared;
- explain the rights of individuals regarding their personal information;
- promote transparency and accountability in the Foundation's handling of personal information;
- demonstrate the Foundation's commitment to ethical data governance and responsible stewardship;
- ensure compliance with applicable data protection and privacy laws; and
- strengthen public confidence in the Foundation's humanitarian, charitable, and community development activities.

This Privacy Policy also provides guidance to donors, volunteers, beneficiaries, partners, grant applicants, suppliers, contractors, employees, and website visitors regarding their relationship with the Foundation in matters concerning privacy and personal information.

3. ABOUT PNEUMA AFRICAN FOUNDATION

Pneuma African Foundation is an international civil society organization dedicated to transforming lives and empowering vulnerable communities throughout Africa. The Foundation exists to promote sustainable community development, humanitarian assistance, health promotion, education, environmental stewardship, human rights, food security, and socio-economic empowerment, with a particular focus on vulnerable island and landing site communities while also serving rural, urban, and other underserved populations across the continent. This mission, vision, and purpose are reflected in the Foundation's governing profile.

The Foundation works collaboratively with governments, development partners, community organisations, faith communities, volunteers, donors, philanthropic institutions, corporations, and international agencies to implement programmes that restore dignity, improve well-being, and create sustainable opportunities for individuals and communities.

In fulfilling this mission, the Foundation necessarily processes personal information relating to donors, volunteers, beneficiaries, employees, partners, consultants, suppliers, applicants, and other stakeholders. The Foundation acknowledges that such information is entrusted to it for legitimate purposes only and must therefore be protected through appropriate governance, security, and ethical standards.

4. OUR COMMITMENT TO PRIVACY

Pneuma African Foundation is committed to maintaining the highest standards of privacy, confidentiality, and information security.

Accordingly, the Foundation commits that it will:

- collect only the personal information that is reasonably necessary for legitimate organisational purposes;
- process personal information lawfully, fairly, and transparently;
- inform individuals how their information is collected and used;
- implement appropriate administrative, technical, and organisational safeguards to protect personal information;
- respect the rights of individuals regarding their personal information;
- ensure that information is not retained longer than necessary;
- never sell personal information to third parties;
- disclose personal information only where authorised by law, by the individual concerned, or where necessary to fulfil legitimate organisational purposes; and
- continuously review and improve its privacy practices to address emerging legal, technological, and operational developments.

Privacy protection is a shared responsibility. Every director, employee, volunteer, consultant, intern, contractor, and representative acting on behalf of Pneuma African Foundation is expected to uphold the standards established in this Policy and to handle personal information with professionalism, integrity, and respect.

5. SCOPE AND APPLICATION

This Privacy Policy applies to all personal information processed by Pneuma African Foundation through any of its activities or systems, including but not limited to:

- the Foundation's official website;
- online donation platforms;

- volunteer recruitment and management;
- grant application processes;
- employment and internship applications;
- fundraising campaigns;
- humanitarian and development programmes;
- beneficiary registration and programme delivery;
- community outreach activities;
- health and medical outreach initiatives;
- training programmes and workshops;
- conferences and events;
- newsletters and mailing lists;
- surveys and research activities;
- social media platforms administered by the Foundation;
- telephone, email, and written correspondence;
- digital applications and online forms; and
- any future digital platforms operated by or on behalf of the Foundation.

This Policy applies regardless of whether personal information is processed electronically, in paper records, verbally, through mobile applications, cloud services, databases, or any other information management system used by the Foundation.

6. DEFINITIONS

For the purposes of this Privacy Policy:

"Personal Information" means any information that identifies or can reasonably be used to identify a living individual, whether directly or indirectly.

"Sensitive Personal Information" means information relating to an individual's health, disability, ethnicity, religion, biometric data, financial information, criminal history, or any other category of information requiring enhanced protection under applicable law.

"Processing" means any operation performed on personal information, including collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure, transmission, restriction, deletion, destruction, or any combination of these activities.

"Data Subject" means the individual to whom personal information relates.

"Website" means the official website of Pneuma African Foundation together with any related digital platforms operated by or on behalf of the Foundation.

"Volunteer" means any individual providing services to the Foundation without entering into an employment relationship.

"Beneficiary" means any individual, household, community, institution, or organisation receiving services, assistance, support, training, grants, or humanitarian interventions from the Foundation.

"Partner" means any government agency, donor, church, corporation, NGO, academic institution, community organisation, consultant, contractor, or other entity collaborating with the Foundation.

"Third Party" means any natural or legal person other than the Foundation or the individual whose information is being processed.

7. PRIVACY PRINCIPLES

In processing personal information, Pneuma African Foundation shall be guided by the following principles:

1. **Lawfulness** – Personal information shall be processed only where there is a lawful basis.
2. **Fairness** – Information shall be collected and used in ways that are fair, reasonable, and respectful of the rights and expectations of individuals.
3. **Transparency** – Individuals shall be informed about how their personal information is collected and used.
4. **Purpose Limitation** – Personal information shall be collected only for specified, legitimate, and clearly communicated purposes.
5. **Data Minimisation** – Only the minimum amount of personal information necessary for the stated purpose shall be collected.
6. **Accuracy** – Reasonable steps shall be taken to ensure that personal information is accurate, complete, and kept up to date.
7. **Storage Limitation** – Personal information shall not be retained longer than necessary unless required by law or legitimate organisational purposes.
8. **Integrity and Confidentiality** – Appropriate safeguards shall be maintained to protect information against loss, unauthorised access, misuse, alteration, or disclosure.
9. **Accountability** – The Foundation accepts responsibility for complying with this Policy and for demonstrating such compliance through effective governance and oversight.

8. LAWFUL BASIS FOR PROCESSING PERSONAL INFORMATION

8.1 Commitment to Lawful Processing

Pneuma African Foundation is committed to ensuring that all personal information is collected, accessed, processed, stored, disclosed, retained, and disposed of in accordance with applicable laws, internationally recognized privacy principles, and the Foundation's commitment to ethical governance.

The Foundation shall process personal information only where there is a legitimate and lawful basis for doing so. Personal information shall never be collected or used arbitrarily,

excessively, or for purposes that are incompatible with the reason for which it was originally obtained.

Every activity involving personal information must be supported by one or more lawful grounds described in this Policy.

8.2 Lawful Grounds for Processing

Depending on the circumstances, Pneuma African Foundation may process personal information on one or more of the following lawful grounds.

A. Consent

The Foundation may process personal information where an individual has freely, knowingly, and voluntarily given clear consent for a specific purpose.

Examples include, but are not limited to:

- subscribing to newsletters and mailing lists;
- registering for conferences, seminars, or training programmes;
- completing online contact forms;
- applying for volunteer opportunities;
- submitting grant applications;
- participating in surveys or research activities;
- consenting to photography, audio recording, or video recording;
- consenting to receive fundraising or marketing communications where required by law.

Consent shall be obtained through clear and understandable language. Silence, inactivity, or pre-ticked boxes shall not be regarded as valid consent.

Where consent is relied upon, individuals may withdraw their consent at any time. Withdrawal of consent shall not affect the lawfulness of processing undertaken before such withdrawal.

B. Performance of a Contract

The Foundation may process personal information where such processing is necessary for the performance of a contract or in order to take steps requested by an individual before entering into a contractual relationship.

Examples include:

- processing employment applications;
- managing employment relationships;

- administering consultancy agreements;
- managing supplier contracts;
- administering partnership agreements;
- processing volunteer agreements;
- administering scholarship programmes;
- organising training services;
- fulfilling grant agreements.

Only information reasonably necessary to fulfil contractual obligations shall be processed.

C. Compliance with Legal Obligations

The Foundation may process personal information where required to comply with applicable laws, regulations, court orders, government directives, audit requirements, taxation laws, financial reporting obligations, anti-money laundering measures, or lawful requests from competent authorities.

Examples include:

- financial audits;
- statutory reporting;
- tax compliance;
- employment obligations;
- anti-fraud investigations;
- safeguarding investigations;
- compliance with court orders;
- reporting suspected criminal activities where required by law.

Where disclosure is legally required, the Foundation shall disclose only the information necessary to comply with the applicable legal obligation.

D. Protection of Vital Interests

Personal information may be processed where necessary to protect the life, health, safety, or physical well-being of an individual or another person.

This lawful basis may arise during:

- humanitarian emergencies;
- medical outreach programmes;
- disaster response operations;
- evacuation procedures;
- emergency referrals;
- child protection interventions;
- safeguarding investigations;
- protection of vulnerable adults.

Where reasonably practicable, the Foundation shall inform affected individuals of such processing after the emergency has passed.

E. Legitimate Interests

The Foundation may process personal information where such processing is necessary for its legitimate organisational interests, provided those interests do not override the fundamental rights and freedoms of the individual.

Legitimate interests may include:

- administering charitable programmes;
- improving service delivery;
- preventing fraud;
- maintaining organisational security;
- protecting Foundation assets;
- responding to enquiries;
- conducting internal audits;
- measuring programme effectiveness;
- evaluating project outcomes;
- maintaining donor relationships;
- communicating organisational updates;
- conducting organisational planning;
- managing risks;
- improving website performance;
- protecting beneficiaries from abuse or exploitation.

Before relying upon legitimate interests, the Foundation shall carefully assess whether the proposed processing is necessary, proportionate, and respectful of individual privacy rights.

F. Public Interest and Humanitarian Purposes

As a humanitarian and community development organisation, Pneuma African Foundation may process personal information where necessary to fulfil its charitable mission and activities carried out in the public interest.

Such activities may include:

- delivering humanitarian assistance;
- community health programmes;
- educational initiatives;
- disaster preparedness;
- emergency relief;
- food security programmes;
- environmental initiatives;
- livelihood development;

- child protection programmes;
- women's empowerment projects;
- disability inclusion programmes;
- community development interventions;
- public awareness campaigns;
- research supporting programme improvement.

Such processing shall always be proportionate, ethical, and consistent with the Foundation's humanitarian mandate. This reflects the Foundation's stated mission to transform and empower vulnerable communities through sustainable development and humanitarian interventions.

8.3 Processing of Sensitive Personal Information

Certain activities undertaken by Pneuma African Foundation may require the processing of sensitive personal information.

Sensitive personal information shall receive enhanced protection and may include:

- medical records;
- disability information;
- health assessments;
- nutritional status;
- biometric information where authorised;
- photographs identifying vulnerable individuals;
- safeguarding records;
- child protection reports;
- ethnicity where required for programme delivery;
- religious affiliation where voluntarily disclosed;
- emergency contact information;
- financial hardship assessments;
- background screening information.

The Foundation shall process sensitive personal information only where:

- explicit consent has been obtained;
- processing is required by law;
- processing is necessary to protect vital interests;
- processing supports legitimate humanitarian objectives;
- appropriate safeguards are implemented.

Access to sensitive information shall be strictly limited to authorised personnel with a legitimate operational need.

8.4 Special Protection for Children and Vulnerable Persons

Because Pneuma African Foundation works extensively with children, women, older persons, persons with disabilities, displaced populations, and other vulnerable communities, the Foundation recognises that information relating to such individuals requires heightened protection.

Accordingly:

- children's information shall receive enhanced safeguards;
- safeguarding records shall remain confidential;
- photographs of children shall only be used in accordance with applicable safeguarding procedures and appropriate consent requirements;
- information relating to abuse, exploitation, neglect, trafficking, or protection concerns shall be handled with the highest degree of confidentiality;
- access to such information shall be restricted to authorised personnel involved in safeguarding or programme delivery.

These commitments are consistent with the Foundation's safeguarding principles and its commitment to protecting vulnerable beneficiaries.

8.5 Fair and Transparent Processing

Whenever personal information is collected directly from an individual, Pneuma African Foundation shall, wherever reasonably practicable, provide information regarding:

- the identity of the Foundation;
- the purpose for which the information is being collected;
- whether providing the information is voluntary or mandatory;
- the lawful basis for processing;
- potential recipients of the information;
- applicable retention periods;
- available privacy rights;
- how to contact the Foundation regarding privacy matters.

Privacy notices shall be written in clear, understandable language that is accessible to the intended audience.

8.6 Purpose Limitation

Personal information collected by the Foundation shall be used only for the specific purposes communicated to the individual at the time of collection or for other compatible purposes permitted by law.

The Foundation shall not use personal information for unrelated purposes without obtaining additional consent or identifying another lawful basis for such processing.

Where the Foundation wishes to use existing information for a materially different purpose, individuals shall be informed before such processing begins unless an applicable law provides otherwise.

8.7 Data Minimisation

Pneuma African Foundation shall collect only the personal information that is adequate, relevant, and reasonably necessary to achieve the intended purpose.

The Foundation shall avoid collecting excessive, unnecessary, or irrelevant information.

Programme managers, staff members, volunteers, consultants, and contractors are expected to ensure that information collection forms, online applications, surveys, and registration processes request only information required for legitimate organisational purposes.

8.8 Accountability for Lawful Processing

The Board of Directors, Executive Management, employees, volunteers, consultants, contractors, and all individuals acting on behalf of Pneuma African Foundation share responsibility for ensuring that personal information is processed lawfully and in accordance with this Privacy Policy.

The Foundation shall maintain appropriate governance structures, internal controls, training programmes, and monitoring mechanisms to promote compliance with this Policy and applicable data protection requirements.

Failure to comply with these requirements may result in disciplinary action, termination of contractual relationships, reporting to competent authorities where appropriate, and any other measures necessary to protect the rights of individuals and the integrity of the Foundation.

9. CATEGORIES OF PERSONAL INFORMATION WE COLLECT

9.1 Introduction

Pneuma African Foundation collects and processes personal information only to the extent necessary to fulfil its charitable mission, humanitarian programmes, governance responsibilities, legal obligations, fundraising activities, volunteer engagement, partnerships, and the effective operation of its website and digital services.

The categories of personal information collected will vary depending on the nature of an individual's relationship with the Foundation. Not every individual will provide every category of information described in this section. The Foundation is committed to collecting only information that is relevant, proportionate, and necessary for the stated purpose.

Where additional categories of information become necessary due to changes in programmes, technology, or legal requirements, this Privacy Policy will be updated accordingly.

9.2 Personal Identification Information

The Foundation may collect information that identifies an individual directly.

This may include:

- Full name
- Previous names where relevant
- Title (Mr., Mrs., Ms., Dr., Rev., Pastor, etc.)
- Gender
- Date of birth
- Nationality
- National Identification Number (where legally required)
- Passport Number (for international programmes)
- Refugee or asylum documentation where applicable
- Driver's licence details where necessary
- Digital identity verification information
- Signature
- Photographs used for identification
- Membership or beneficiary identification numbers issued by the Foundation

This information is collected for purposes including identity verification, programme administration, safeguarding, legal compliance, volunteer management, employment, and donor administration.

9.3 Contact Information

The Foundation may collect information necessary for communication.

This includes:

- Residential address
- Postal address
- Business address
- Email address
- Telephone number

- Mobile number
- WhatsApp number
- Emergency contact details
- Next of kin information
- Preferred language
- Preferred communication method

This information enables the Foundation to communicate effectively with donors, beneficiaries, volunteers, partners, suppliers, and other stakeholders.

9.4 Website and Technical Information

When individuals visit the Foundation's website, certain technical information may be collected automatically to support website functionality, security, and performance.

This may include:

- Internet Protocol (IP) address
- Browser type and version
- Device type
- Operating system
- Screen resolution
- Language preferences
- Date and time of access
- Referring website
- Pages visited
- Downloads
- Session duration
- Clickstream data
- Search terms used within the website
- Error logs
- Cookies and similar technologies
- Security logs
- Device identifiers

This information assists the Foundation in maintaining website security, diagnosing technical issues, improving user experience, and understanding how visitors interact with the website.

9.5 Donation Information

Individuals who support the Foundation financially may provide information necessary for processing donations and maintaining accurate donor records.

Donation information may include:

- Donor name
- Contact details
- Donation amount
- Currency
- Donation frequency
- Payment confirmation
- Transaction reference
- Gift Aid or tax-related declarations where applicable
- Donation purpose
- Restricted or unrestricted donation preferences
- Sponsorship information
- Campaign participation
- Employer matching information
- Communication preferences
- Donation history

The Foundation uses this information to acknowledge donations, maintain financial records, comply with applicable financial regulations, provide receipts where appropriate, communicate with donors, and ensure accountability in the stewardship of donated resources.

The Foundation does not intentionally store complete payment card details on its own systems where secure third-party payment service providers are used.

9.6 Payment Information

Where payments are made through the Foundation's website or authorised fundraising platforms, payment-related information may be processed.

Depending upon the payment method, this may include:

- Payment confirmation
- Payment status
- Transaction identifier
- Payment date
- Payment method
- Bank transfer reference
- Mobile money transaction reference
- Digital wallet confirmation
- Financial institution involved

Sensitive payment credentials are processed by secure payment service providers operating under their own security and compliance obligations.

9.7 Volunteer Information

Individuals applying to volunteer with the Foundation may provide information including:

- Personal profile
- Educational background
- Professional qualifications
- Curriculum Vitae (CV)
- Employment history
- Skills
- Languages spoken
- Areas of interest
- Volunteer availability
- Emergency contacts
- References
- Background verification information
- Safeguarding declarations
- Medical information relevant to volunteer safety
- Travel documentation where necessary

Volunteer information is used for recruitment, placement, safeguarding, supervision, training, welfare, insurance, programme management, and compliance with applicable legal and organisational requirements. These uses align with the Foundation's volunteer engagement practices.

9.8 Beneficiary Information

In delivering humanitarian assistance and community development programmes, the Foundation may collect personal information relating to beneficiaries.

Depending on the programme, this may include:

- Household composition
- Family relationships
- Age
- Gender
- Community location
- Vulnerability assessments
- Disability information
- Educational information
- Livelihood information
- Income assessments
- Health information where relevant
- Nutritional assessments
- Agricultural information
- Housing information
- Programme participation history
- Monitoring and evaluation information
- Case management information

- Emergency assistance records

The Foundation collects only information necessary for effective programme delivery, monitoring, safeguarding, reporting, and accountability to donors and regulatory authorities.

9.9 Children's Information

Because the Foundation undertakes programmes involving children and young people, limited personal information relating to children may be collected where necessary.

Such information may include:

- Child's name
- Date of birth
- Age
- Gender
- School information
- Parent or guardian information
- Emergency contacts
- Health considerations relevant to programme participation
- Safeguarding records
- Programme participation records
- Child protection reports
- Educational support information

The Foundation recognises that children's personal information requires enhanced protection and shall implement appropriate safeguarding measures in accordance with its Child Protection and Safeguarding Policies.

9.10 Health Information

Certain Foundation programmes may require the collection of limited health-related information.

Examples include:

- Disability status
- Allergies
- Medical conditions relevant to programme participation
- Emergency medical information
- Nutritional assessments
- Vaccination information where required by law or programme needs
- Accessibility requirements
- Mental health support requirements where voluntarily disclosed

Health information shall be treated as sensitive personal information and shall receive enhanced protection.

9.11 Employment and Recruitment Information

Individuals applying for employment with the Foundation may provide:

- Employment applications
- Academic qualifications
- Professional licences
- References
- Criminal background checks where permitted by law
- Employment history
- Salary expectations
- Interview notes
- Assessment results
- Identity verification documents

Information collected during recruitment will be processed solely for recruitment, employment, legal compliance, and human resource administration.

9.12 Partner and Supplier Information

The Foundation may collect information relating to organisations and individuals providing goods or services.

This may include:

- Organisation name
- Business registration details
- Contact persons
- Banking information
- Tax registration numbers
- Contract information
- Procurement documentation
- Compliance certifications
- Insurance information
- Performance records

This information is required for procurement, contracting, financial management, due diligence, and partnership administration.

9.13 Grant Applicants and Project Partners

Organisations and individuals applying for grants or project partnerships may provide:

- Organisational profiles
- Project proposals
- Financial statements
- Governance documents
- Bank account information
- Monitoring reports
- Project evaluations
- Contact details
- References
- Due diligence documentation

The Foundation uses this information to assess eligibility, administer funding, monitor projects, and ensure responsible stewardship of charitable resources.

9.14 Event Registration Information

Individuals attending Foundation events, conferences, workshops, seminars, or training programmes may provide:

- Registration details
- Attendance records
- Dietary requirements
- Accessibility requirements
- Travel arrangements
- Accommodation information where organised by the Foundation
- Certificates issued
- Emergency contacts

This information enables the Foundation to organise safe, inclusive, and effective events.

9.15 Communications Information

The Foundation may retain records of communications with individuals, including:

- Emails
- Letters
- Telephone call records where lawfully maintained

- Online enquiries
- Contact form submissions
- Social media messages
- Complaints
- Feedback
- Survey responses
- Requests for information

These records assist the Foundation in responding to enquiries, resolving issues, improving services, and maintaining accurate organisational records.

9.16 Photographs, Audio and Video Recordings

The Foundation may collect or create visual and audio materials for legitimate organisational purposes, including:

- Programme documentation
- Project monitoring
- Donor reporting
- Awareness campaigns
- Educational materials
- Publications
- Newsletters
- Annual reports
- Website content
- Social media communications

Where required by law or organisational policy, appropriate consent will be obtained before using identifiable photographs, audio recordings, or video recordings. Special care shall be taken when recording or publishing images of children and vulnerable persons.

9.17 Information We Do Not Intentionally Collect

The Foundation does not intentionally collect personal information that is unnecessary for its legitimate activities.

In particular, the Foundation does not intentionally:

- collect excessive personal information;
- sell personal information to third parties;

- collect payment card security codes for storage;
 - collect sensitive personal information without an appropriate lawful basis;
 - monitor private communications unrelated to Foundation activities; or
 - engage in automated profiling or decision-making that produces legal or similarly significant effects on individuals without appropriate safeguards.
-

9.18 Accuracy and Updating of Personal Information

The Foundation relies on individuals to provide accurate, complete, and up-to-date information.

Individuals are encouraged to notify the Foundation promptly if:

- their contact details change;
- their legal name changes;
- emergency contacts require updating;
- inaccurate information has been recorded; or
- they wish to correct or update information previously provided.

The Foundation will take reasonable steps to ensure that personal information remains accurate and current for the purposes for which it is processed.

10. HOW WE COLLECT PERSONAL INFORMATION

10.1 Introduction

Pneuma African Foundation collects personal information through lawful, fair, transparent, and secure means in order to carry out its charitable, humanitarian, development, governance, fundraising, advocacy, volunteer management, and administrative activities.

The Foundation is committed to ensuring that individuals understand how their personal information is obtained and that information is collected only where there is a legitimate organisational purpose and a lawful basis for processing.

Personal information may be collected directly from individuals, indirectly through authorised third parties, automatically through the Foundation's digital platforms, or through other lawful means described in this Policy.

The Foundation does not obtain personal information through deceptive, misleading, unlawful, or unethical practices.

10.2 Information Collected Directly from Individuals

The majority of personal information processed by the Foundation is collected directly from the individual concerned.

Information may be provided when an individual:

- makes a donation;
- registers as a volunteer;
- applies for employment;
- submits a grant application;
- becomes a programme beneficiary;
- registers for conferences, workshops, seminars, or training programmes;
- subscribes to newsletters;
- requests publications or educational materials;
- contacts the Foundation by email, telephone, social media, or through the website;
- completes surveys, questionnaires, or research activities;
- requests humanitarian assistance;
- participates in Foundation projects or community programmes;
- enters into contracts with the Foundation; or
- otherwise communicates with the Foundation.

Where information is collected directly, the Foundation shall, wherever reasonably practicable, explain:

- why the information is being collected;
- how it will be used;
- who may receive it;
- how long it may be retained; and
- the rights available to the individual under this Privacy Policy.

10.3 Information Collected Through the Foundation's Website

The Foundation's website serves as an important platform for communication, education, fundraising, programme information, volunteer engagement, and stakeholder interaction.

When individuals visit the website, information may be collected through:

- online forms;
- donation forms;

- volunteer registration forms;
- event registration pages;
- newsletter subscription forms;
- contact forms;
- grant application portals;
- downloadable publication requests;
- user account registration where applicable;
- feedback forms;
- survey forms;
- technical website logs;
- cookies and similar technologies;
- website analytics tools.

Information collected through the website is used to improve website functionality, enhance user experience, provide requested services, maintain website security, and support the Foundation's charitable mission.

10.4 Information Collected During Donations

When individuals make financial contributions to the Foundation, personal information may be collected during the donation process.

Depending on the donation method, this information may include:

- donor identification details;
- contact information;
- donation amount;
- payment confirmation;
- transaction reference numbers;
- preferred designation of donated funds;
- recurring donation preferences;
- communication preferences;
- tax-related information where applicable.

Donation information enables the Foundation to:

- process donations securely;
- acknowledge contributions;
- issue receipts where appropriate;
- maintain financial records;
- comply with legal and regulatory obligations;
- provide donor support;
- report appropriately on restricted funding where applicable.

Payment information is collected through secure payment systems approved by the Foundation.

10.5 Information Collected During Volunteer Recruitment

Individuals expressing interest in volunteering with Pneuma African Foundation may voluntarily submit personal information through application forms, interviews, orientation sessions, background verification processes, safeguarding declarations, training programmes, and related communications.

This information assists the Foundation in:

- assessing suitability;
- matching volunteers with appropriate programmes;
- ensuring safeguarding compliance;
- managing volunteer welfare;
- coordinating assignments;
- maintaining emergency contacts;
- fulfilling legal and insurance obligations.

Volunteer information is collected only to the extent necessary for responsible volunteer management and safeguarding. These practices support the Foundation's volunteer programme framework.

10.6 Information Collected During Programme Delivery

As part of its humanitarian and development work, the Foundation may collect information from beneficiaries and participating communities.

Information may be collected through:

- beneficiary registration;
- household assessments;
- community surveys;
- needs assessments;
- vulnerability assessments;
- programme enrolment;
- monitoring visits;
- evaluation activities;
- health outreach programmes;

- educational initiatives;
- livelihood programmes;
- environmental projects;
- humanitarian response activities;
- community meetings.

Information collected during programme implementation is used solely for legitimate programme planning, delivery, safeguarding, monitoring, evaluation, reporting, accountability, and organisational learning.

10.7 Information Collected During Employment and Recruitment

Applicants for employment, internships, consultancy assignments, or contractual engagements may provide personal information during recruitment.

Information may be collected through:

- application forms;
- curriculum vitae;
- interviews;
- professional references;
- academic verification;
- identity verification;
- employment assessments;
- background screening where permitted by law.

Recruitment information shall be used exclusively for employment-related purposes and managed in accordance with applicable legal and organisational requirements.

10.8 Information Collected During Events and Training

The Foundation regularly organises conferences, workshops, seminars, leadership training, community sensitisation programmes, fundraising events, and public awareness campaigns.

Information may be collected during:

- event registration;
- attendance confirmation;
- participant sign-in;
- certification processes;

- post-event evaluations;
- feedback surveys;
- networking activities.

Such information assists the Foundation in organising events effectively, ensuring participant safety, improving future programmes, and maintaining accurate organisational records.

10.9 Information Collected Through Communications

The Foundation may collect personal information whenever individuals communicate with the organisation.

This includes communications received through:

- email;
- telephone;
- postal mail;
- social media platforms;
- messaging applications;
- website contact forms;
- online chat systems where available;
- in-person meetings;
- community outreach activities.

Records of communications may be maintained where necessary to respond appropriately, resolve concerns, improve services, fulfil legal obligations, or protect the legitimate interests of the Foundation and the individuals involved.

10.10 Information Collected Through Cookies and Similar Technologies

The Foundation's website may automatically collect limited technical information using cookies, pixels, log files, and similar technologies.

These technologies may collect information relating to:

- browsing activity;
- session information;
- device characteristics;
- browser preferences;
- website performance;

- language settings;
- security monitoring;
- website analytics.

Such technologies assist the Foundation in improving website performance, enhancing user experience, preventing fraud, maintaining cybersecurity, and understanding how visitors use the website.

Detailed information regarding cookies is provided in the Foundation's Cookie Policy.

10.11 Information Obtained from Third Parties

In certain circumstances, the Foundation may lawfully receive personal information from authorised third parties.

Such third parties may include:

- payment service providers;
- financial institutions;
- government agencies;
- educational institutions;
- employers providing volunteer references;
- partner organisations;
- humanitarian agencies;
- grant-making organisations;
- community leaders;
- healthcare providers where authorised;
- safeguarding agencies;
- law enforcement authorities;
- publicly available official records.

Where information is received from third parties, the Foundation shall take reasonable steps to ensure that:

- the third party was authorised to provide the information;
 - the information was obtained lawfully;
 - the information is relevant and accurate;
 - appropriate privacy protections are maintained.
-

10.12 Information from Publicly Available Sources

The Foundation may obtain limited information from publicly available sources where there is a legitimate organisational purpose.

Such sources may include:

- government registries;
- charity registers;
- company registers;
- professional directories;
- publicly accessible organisational websites;
- publicly available publications;
- media reports;
- publicly available social media profiles where relevant to Foundation activities.

Information obtained from public sources shall be used responsibly and only for legitimate purposes consistent with this Privacy Policy.

10.13 Photographs, Audio Recordings and Video Recordings

The Foundation may collect photographs, audio recordings, or video recordings during its programmes, events, outreach activities, humanitarian operations, fundraising campaigns, or public awareness initiatives.

These materials may be collected for purposes including:

- documenting programme activities;
- donor accountability;
- annual reporting;
- educational publications;
- advocacy campaigns;
- fundraising materials;
- website content;
- newsletters;
- social media communications;
- organisational archives.

Where required by law or organisational policy, informed consent will be obtained before recording or publishing identifiable individuals. Additional safeguards shall apply when children or vulnerable persons are involved, consistent with the Foundation's safeguarding commitments.

10.14 Information Generated During Foundation Activities

Some personal information is generated as individuals interact with the Foundation over time.

Examples include:

- programme participation history;
- volunteer service records;
- training certificates;
- donor history;
- communication records;
- complaint records;
- safeguarding reports;
- audit findings;
- monitoring reports;
- project evaluations;
- recognition awards;
- attendance records.

Such information forms part of the Foundation's legitimate operational records and shall be managed in accordance with this Privacy Policy and applicable records management requirements.

10.15 Accuracy of Information Collected

The Foundation encourages individuals to provide accurate, complete, and current information.

Reasonable measures shall be taken to:

- verify information where appropriate;
- correct inaccurate information;
- update records when changes are reported;
- remove duplicate records;
- minimise errors during data collection.

Where inaccuracies are identified, the Foundation shall correct them without undue delay, subject to appropriate verification.

10.16 Collection Limitation

The Foundation shall collect only the minimum amount of personal information reasonably necessary to achieve the specific purpose for which the information is collected.

The Foundation shall not knowingly:

- collect excessive personal information;
- request irrelevant information;
- use deceptive collection methods;
- collect information without a legitimate organisational purpose;
- retain unnecessary information after the purpose for collection has ended.

All data collection activities shall be guided by the principles of necessity, proportionality, fairness, transparency, accountability, and respect for the rights and dignity of every individual.

10.17 Commitment to Ethical Information Collection

Pneuma African Foundation is committed to maintaining public trust through responsible and ethical information collection practices.

Accordingly, the Foundation shall:

- collect information honestly and transparently;
- respect the privacy and dignity of every individual;
- avoid unnecessary intrusion into private affairs;
- provide appropriate privacy notices at the point of collection;
- protect information throughout its lifecycle; and
- continuously review its collection practices to ensure compliance with applicable laws, recognised privacy standards, and the Foundation's governance framework.

By adhering to these principles, the Foundation seeks to foster confidence among donors, beneficiaries, volunteers, employees, partners, and the communities it serves.

11. HOW WE USE PERSONAL INFORMATION

11.1 Introduction

Pneuma African Foundation processes personal information solely for legitimate, lawful, ethical, and mission-driven purposes that support its humanitarian, charitable, educational, development, governance, and operational activities.

The Foundation shall use personal information only for purposes that are compatible with the reason for which the information was originally collected, unless a further lawful basis exists or the individual has provided additional consent where required.

Personal information shall never be used in a manner that is unfair, discriminatory, deceptive, or inconsistent with the Foundation's values of integrity, accountability, transparency, respect for human dignity, and responsible stewardship.

The Foundation is committed to ensuring that every use of personal information is proportionate, necessary, secure, and consistent with applicable laws and this Privacy Policy.

11.2 Programme Planning and Service Delivery

One of the Foundation's principal purposes for processing personal information is to plan, implement, monitor, evaluate, and improve humanitarian, charitable, and community development programmes.

Personal information may be used to:

- assess community needs;
- identify programme beneficiaries;
- determine eligibility for assistance;
- deliver humanitarian support;
- coordinate relief interventions;
- implement education programmes;
- facilitate health outreach initiatives;
- administer livelihood programmes;
- support food security initiatives;
- implement environmental conservation projects;
- provide women's empowerment services;
- facilitate youth development programmes;
- promote disability inclusion;
- strengthen community resilience;
- monitor programme participation;
- evaluate programme outcomes;
- measure community impact.

These activities directly support the Foundation's mission of transforming vulnerable communities through sustainable development and humanitarian interventions.

11.3 Administration of Donations

Personal information relating to donors is used to ensure the transparent, accurate, and accountable administration of charitable contributions.

Donation information may be used to:

- process donations;
- verify transactions;
- issue acknowledgements and receipts;
- administer recurring donations;
- maintain donor records;
- respond to donor enquiries;
- manage designated or restricted donations;
- prepare financial reports;
- comply with accounting requirements;
- recognise donor support where appropriate and with consent;
- maintain audit records;
- prevent fraud and financial abuse.

The Foundation is committed to ensuring that donor information is treated with confidentiality and used only for legitimate fundraising and stewardship purposes.

11.4 Communication with Donors, Supporters, and Stakeholders

The Foundation may use personal information to communicate with individuals regarding matters relevant to their relationship with the organisation.

Communications may include:

- donation acknowledgements;
- programme updates;
- newsletters;
- annual reports;
- humanitarian appeals;
- fundraising campaigns;
- invitations to Foundation events;
- volunteer opportunities;
- policy updates;
- governance notices;
- organisational announcements;
- responses to enquiries;
- customer support.

Individuals may opt out of non-essential communications at any time using the methods provided in the communication or by contacting the Foundation directly.

11.5 Volunteer Recruitment and Management

Personal information provided by volunteers and volunteer applicants may be used to:

- evaluate volunteer applications;
- conduct interviews;
- verify references;
- undertake safeguarding checks where appropriate;
- assign volunteers to suitable programmes;
- organise volunteer training;
- maintain attendance records;
- coordinate volunteer schedules;
- administer insurance requirements;
- manage emergency contacts;
- evaluate volunteer performance;
- recognise volunteer contributions;
- ensure volunteer safety and welfare.

These activities support the Foundation's volunteer programme and its commitment to effective volunteer engagement and safeguarding.

11.6 Safeguarding and Protection

The Foundation may process personal information where necessary to safeguard children, vulnerable adults, beneficiaries, volunteers, staff, and community members.

Such processing may include:

- investigating safeguarding concerns;
- responding to reports of abuse;
- managing child protection cases;
- assessing risks;
- documenting safeguarding incidents;
- cooperating with competent authorities;
- implementing protective measures;
- supporting affected individuals;
- monitoring safeguarding compliance.

Safeguarding information shall be handled with strict confidentiality and shall be accessible only to authorised personnel with a legitimate need to know.

The Foundation's safeguarding commitments are reflected in its Code of Conduct and related governance documents.

11.7 Employment and Human Resource Administration

Where individuals are employed or engaged by the Foundation, personal information may be processed to:

- recruit staff;
- administer employment contracts;
- manage payroll;
- administer employee benefits;
- assess performance;
- provide training;
- maintain personnel records;
- comply with employment legislation;
- ensure workplace health and safety;
- administer leave;
- manage disciplinary procedures;
- support professional development.

Employment-related information shall be processed only for legitimate human resource purposes.

11.8 Financial Management and Accountability

Personal information may be used to support responsible financial management and accountability.

This includes:

- maintaining accounting records;
- preparing budgets;
- conducting financial audits;
- processing payments;
- reconciling transactions;
- administering grants;
- ensuring donor accountability;
- complying with financial reporting obligations;
- preventing fraud;

- managing procurement processes.

These activities support the Foundation's commitment to transparency and responsible stewardship of charitable resources.

11.9 Compliance with Legal and Regulatory Obligations

The Foundation may process personal information where necessary to comply with applicable laws, regulations, court orders, regulatory requirements, or lawful requests from competent authorities.

Examples include:

- taxation requirements;
- employment law obligations;
- charity governance requirements;
- financial reporting;
- audit obligations;
- anti-money laundering compliance;
- fraud investigations;
- safeguarding reporting obligations;
- responses to lawful judicial or governmental requests.

Only the minimum amount of information necessary to satisfy the relevant legal obligation shall be disclosed.

11.10 Website Administration and Security

Personal information and technical information collected through the Foundation's website may be used to:

- maintain website functionality;
- improve website performance;
- detect security threats;
- prevent cyberattacks;
- monitor website usage;
- diagnose technical issues;
- improve accessibility;
- prevent unauthorised access;
- investigate misuse of the website;
- enhance user experience.

Website security remains an essential component of protecting both the Foundation and individuals interacting with its digital services.

11.11 Research, Monitoring, Evaluation, and Learning

To improve programme quality and organisational effectiveness, the Foundation may process personal information for:

- programme monitoring;
- project evaluation;
- impact assessment;
- organisational learning;
- policy development;
- statistical analysis;
- research studies;
- donor reporting;
- academic collaborations where appropriate;
- measuring community outcomes.

Where practical, the Foundation shall use anonymised or aggregated information for research and reporting to minimise the identification of individuals.

11.12 Communications and Public Awareness

The Foundation may use personal information, photographs, audio recordings, and video recordings for legitimate communications and public awareness purposes.

This may include:

- annual reports;
- newsletters;
- publications;
- educational resources;
- advocacy campaigns;
- fundraising campaigns;
- documentaries;
- website content;
- social media;
- press releases;
- promotional materials.

Where legally required or appropriate, consent shall be obtained before publishing identifiable images or stories. Particular care shall be exercised when featuring children or vulnerable individuals.

11.13 Event Management

Information collected from participants may be used to:

- organise events;
- confirm registrations;
- communicate logistical information;
- issue attendance certificates;
- accommodate accessibility requirements;
- arrange travel or accommodation where applicable;
- improve future events through participant feedback.

The Foundation seeks to ensure that events are organised safely, efficiently, and inclusively.

11.14 Responding to Enquiries and Requests

Personal information may be used to:

- respond to enquiries;
- provide requested information;
- process complaints;
- resolve disputes;
- answer questions regarding Foundation programmes;
- provide technical support;
- facilitate communication with beneficiaries, donors, volunteers, partners, and members of the public.

The Foundation aims to respond to enquiries in a timely, respectful, and professional manner.

11.15 Risk Management and Organisational Governance

Personal information may be processed to support sound governance and organisational oversight.

Examples include:

- internal audits;
- governance reviews;
- risk assessments;
- policy compliance monitoring;
- investigations into misconduct;
- conflict-of-interest management;
- regulatory inspections;
- quality assurance activities.

These processes contribute to effective governance and accountability throughout the Foundation.

11.16 Fraud Prevention and Security

The Foundation may use personal information to:

- detect fraudulent activities;
- investigate financial irregularities;
- prevent misuse of Foundation resources;
- protect beneficiaries;
- verify identities;
- detect duplicate applications;
- prevent cybercrime;
- protect organisational assets;
- support safeguarding investigations.

Where fraud or criminal conduct is suspected, information may be shared with competent authorities in accordance with applicable law.

11.17 Improvement of Foundation Services

The Foundation continually seeks to improve the quality of its services and programmes.

Personal information may therefore be analysed to:

- identify service gaps;
- improve programme delivery;
- strengthen volunteer engagement;
- enhance donor experiences;
- improve beneficiary support;
- evaluate operational effectiveness;
- improve website usability;

- develop new initiatives aligned with the Foundation's mission.

Whenever possible, aggregated or anonymised information shall be used for organisational improvement.

11.18 Record Keeping and Organisational Memory

The Foundation maintains records to ensure continuity, accountability, and effective governance.

Personal information may therefore be retained for purposes including:

- historical organisational records;
- legal compliance;
- financial accountability;
- programme continuity;
- safeguarding documentation;
- governance records;
- audit trails;
- institutional learning.

Records shall be managed in accordance with the Foundation's records management practices and applicable legal requirements.

11.19 Purposes for Which Information Will Not Be Used

Pneuma African Foundation is committed to respecting the privacy and trust of all individuals.

Accordingly, the Foundation shall **not** use personal information to:

- sell personal information to third parties;
- engage in unauthorised commercial marketing unrelated to its mission;
- discriminate unlawfully against any individual;
- exploit vulnerable persons;
- conduct unlawful surveillance;
- process information for purposes incompatible with those communicated at the time of collection without an appropriate lawful basis;
- publish confidential information without authority or legal justification.

11.20 Commitment to Responsible Use of Personal Information

Every director, employee, volunteer, consultant, contractor, intern, and representative acting on behalf of Pneuma African Foundation is responsible for ensuring that personal information is used responsibly, ethically, and in accordance with this Privacy Policy.

The Foundation shall regularly review its information processing activities to ensure that personal information continues to be used only for legitimate, lawful, and mission-aligned purposes.

By maintaining these standards, Pneuma African Foundation seeks to uphold the confidence placed in it by donors, beneficiaries, volunteers, partners, governments, and the communities it serves.

12. WHEN AND HOW WE SHARE PERSONAL INFORMATION

12.1 Introduction

Pneuma African Foundation recognises that personal information entrusted to the Foundation is confidential and must be protected against unauthorised disclosure.

The Foundation does **not** sell, rent, trade, lease, or otherwise commercially exploit personal information. Personal information shall be disclosed only where there is a legitimate organisational need, a lawful basis for disclosure, the consent of the individual where required, or a legal obligation to do so.

Whenever personal information is shared, the Foundation shall take reasonable steps to ensure that the receiving party maintains appropriate standards of confidentiality, privacy, security, and lawful processing consistent with this Privacy Policy.

12.2 General Principles for Information Sharing

The Foundation shall disclose personal information only where such disclosure is:

- lawful;
- necessary;

- proportionate;
- relevant to the intended purpose;
- appropriately authorised;
- adequately documented; and
- protected by appropriate contractual, organisational, or legal safeguards.

The Foundation shall always seek to disclose the minimum amount of personal information necessary to fulfil the specific purpose for which disclosure is required.

12.3 Sharing Within Pneuma African Foundation

Personal information may be shared internally among authorised directors, officers, employees, volunteers, consultants, interns, and contractors where access is necessary for the proper performance of their duties.

Internal access shall be limited on a "need-to-know" basis.

Examples include:

- programme management;
- donor administration;
- volunteer coordination;
- finance;
- safeguarding;
- legal compliance;
- information technology;
- communications;
- human resources;
- governance functions.

All persons with access to personal information are required to maintain confidentiality and comply with this Privacy Policy and other applicable Foundation policies.

12.4 Sharing with Service Providers

The Foundation may engage trusted third-party service providers to support its operations.

Examples include providers of:

- website hosting;
- cloud storage;
- email services;

- payment processing;
- accounting systems;
- customer relationship management (CRM) platforms;
- cybersecurity services;
- information technology support;
- data backup services;
- document management;
- communications platforms;
- event management systems.

Where third-party service providers process personal information on behalf of the Foundation, they shall be required, through appropriate contractual arrangements where applicable, to:

- process personal information only for authorised purposes;
- maintain appropriate security measures;
- protect confidentiality;
- comply with applicable data protection laws;
- notify the Foundation of relevant security incidents where required;
- return or securely dispose of personal information upon completion of their services, where appropriate.

Service providers shall not be authorised to use personal information for their own marketing or unrelated commercial purposes.

12.5 Sharing with Payment Service Providers

Where donations or payments are processed electronically, relevant personal information may be shared with authorised payment service providers.

Information shared may include:

- donor identification details;
- payment amount;
- transaction references;
- payment confirmations;
- billing information where required;
- fraud prevention information.

Payment providers process information under their own privacy and security obligations.

The Foundation shall use reputable payment providers that implement appropriate safeguards for financial transactions.

12.6 Sharing with Banking and Financial Institutions

The Foundation may disclose relevant information to banks and financial institutions where necessary to:

- process donations;
- receive grant funding;
- administer payroll;
- process supplier payments;
- investigate fraudulent transactions;
- comply with financial regulations;
- complete financial reconciliations.

Only information reasonably necessary for these purposes shall be disclosed.

12.7 Sharing with Government Authorities and Regulators

The Foundation may disclose personal information where required by applicable law or lawful requests from competent authorities.

Examples include:

- taxation authorities;
- charity regulators;
- financial regulators;
- labour authorities;
- immigration authorities;
- public health authorities;
- courts;
- law enforcement agencies;
- anti-corruption agencies.

Before disclosing personal information, the Foundation shall, where legally permissible, verify the legitimacy of the request and ensure that only the minimum necessary information is provided.

12.8 Sharing for Safeguarding and Protection Purposes

The safety and protection of children, vulnerable adults, beneficiaries, volunteers, staff, and community members is of paramount importance.

Accordingly, the Foundation may disclose relevant personal information where necessary to:

- protect a child from harm;
- investigate abuse;
- respond to safeguarding concerns;
- prevent exploitation;
- report suspected criminal conduct;
- cooperate with child protection authorities;
- protect vulnerable adults;
- respond to emergency situations.

Such disclosures shall be made only to authorised agencies or individuals with legitimate safeguarding responsibilities and in accordance with applicable law and the Foundation's safeguarding commitments.

12.9 Sharing with Programme Partners

The Foundation frequently collaborates with governments, community organisations, faith-based organisations, academic institutions, humanitarian agencies, and development partners.

Where programme delivery requires collaboration, limited personal information may be shared with authorised partners for purposes including:

- programme implementation;
- beneficiary referrals;
- project coordination;
- monitoring and evaluation;
- grant administration;
- community development initiatives;
- capacity-building programmes;
- humanitarian response.

Programme partners shall receive only the information necessary for their role and shall be expected to maintain appropriate confidentiality and data protection standards.

12.10 Sharing with Auditors and Professional Advisers

The Foundation may disclose relevant information to independent professionals engaged to support its governance and legal obligations.

This may include:

- external auditors;
- internal auditors;
- legal advisers;
- accountants;
- tax advisers;
- governance consultants;
- risk management advisers.

Such professionals shall be required to maintain appropriate confidentiality in accordance with professional obligations and applicable law.

12.11 Sharing with Insurers

Where necessary, personal information may be disclosed to insurers or insurance brokers for purposes including:

- volunteer insurance;
- employee insurance;
- travel insurance;
- public liability claims;
- accident investigations;
- claims management;
- risk assessments.

Only information relevant to the insurance purpose shall be disclosed.

12.12 Sharing During Emergencies

Where necessary to protect life, health, or safety, the Foundation may disclose relevant personal information during emergencies.

Examples include:

- medical emergencies;
- natural disasters;
- humanitarian crises;
- evacuation procedures;
- missing person investigations;
- public health emergencies.

Emergency disclosures shall be limited to information necessary to protect individuals or communities.

12.13 International Sharing of Personal Information

Because Pneuma African Foundation collaborates with international donors, development agencies, humanitarian partners, churches, philanthropic institutions, and service providers, personal information may occasionally be transferred outside the country in which it was originally collected.

International transfers may occur for purposes including:

- grant administration;
- programme reporting;
- cloud-based information technology services;
- secure data hosting;
- donor reporting;
- international audits;
- collaborative humanitarian programmes;
- technical support.

Where international transfers occur, the Foundation shall take reasonable steps to ensure that appropriate safeguards are implemented to protect personal information.

Further information regarding international data transfers is provided in **Section 13 – International Data Transfers** of this Privacy Policy.

12.14 Sharing During Organisational Restructuring

In the unlikely event of:

- organisational restructuring;
- merger;
- legal reorganisation;
- transfer of programmes;
- establishment of affiliated entities;
- dissolution of the Foundation,

personal information may be transferred where necessary to ensure continuity of lawful operations.

Any successor organisation receiving such information shall be required to continue protecting personal information in accordance with applicable law and this Privacy Policy, or a substantially equivalent standard.

12.15 Information Published with Consent

The Foundation may publish limited personal information where an individual has provided appropriate consent.

Examples include:

- donor recognition lists;
- volunteer awards;
- success stories;
- testimonials;
- event speakers;
- community champions;
- publications;
- newsletters;
- annual reports;
- website content.

Individuals may withdraw consent for future publication where legally applicable, although materials already lawfully published may not always be capable of complete withdrawal from public circulation.

12.16 Information Shared in Aggregated or Anonymised Form

The Foundation may publish or share statistical information that has been anonymised or aggregated so that individuals cannot reasonably be identified.

Examples include:

- programme statistics;
- annual reports;
- donor reports;
- research findings;
- community impact reports;
- monitoring and evaluation summaries;
- strategic planning documents.

Aggregated information does not constitute personal information where individuals cannot reasonably be identified.

12.17 Information We Will Not Share

Except where required by law or authorised under this Privacy Policy, Pneuma African Foundation shall not:

- sell personal information;
- rent personal information;
- trade mailing lists;
- disclose donor information for commercial marketing;
- disclose beneficiary information for commercial gain;
- disclose safeguarding records without lawful authority;
- disclose confidential employee information without appropriate justification;
- publish sensitive personal information without a lawful basis;
- share personal information with unauthorised third parties.

The Foundation is committed to preserving the trust placed in it by donors, beneficiaries, volunteers, partners, employees, and the communities it serves.

12.18 Safeguards Applied to Information Sharing

Whenever personal information is disclosed, the Foundation shall implement appropriate safeguards, which may include:

- confidentiality agreements;
- data processing agreements where appropriate;
- secure electronic transmission;
- encrypted communications where necessary;
- access controls;
- authentication procedures;
- records of disclosures where appropriate;
- staff training;
- organisational policies;
- periodic compliance reviews.

The Foundation shall continuously evaluate its information-sharing practices to ensure that they remain lawful, proportionate, secure, and aligned with recognised standards of good governance.

12.19 Accountability for Information Sharing

The Board of Directors, Executive Management, employees, volunteers, consultants, contractors, and all persons acting on behalf of Pneuma African Foundation are responsible for ensuring that personal information is shared only in accordance with this Privacy Policy.

Unauthorised disclosure of personal information may result in disciplinary action, termination of employment or contractual relationships, reporting to competent authorities where appropriate, and any other lawful measures necessary to protect affected individuals and the integrity of the Foundation.

13. INTERNATIONAL DATA TRANSFERS

13.1 Introduction

Pneuma African Foundation is an international civil society organisation that collaborates with donors, humanitarian agencies, governments, development partners, churches, academic institutions, service providers, volunteers, consultants, and beneficiaries across multiple countries. As part of its mission to transform vulnerable communities through sustainable development and humanitarian action, the Foundation may need to transfer personal information across national borders.

The Foundation recognises that international transfers of personal information require heightened safeguards to ensure that individuals' privacy rights remain protected regardless of where their information is processed or stored.

Accordingly, Pneuma African Foundation is committed to ensuring that all international transfers of personal information are conducted lawfully, securely, transparently, and in accordance with this Privacy Policy and applicable data protection legislation.

13.2 Circumstances in Which International Transfers May Occur

Personal information may be transferred internationally where such transfer is necessary for the legitimate activities of the Foundation.

Examples include:

- administration of international donor-funded programmes;

- collaboration with international humanitarian organisations;
- partnerships with foreign universities and research institutions;
- cross-border volunteer programmes;
- international conferences and training events;
- grant management and reporting;
- cloud-based information technology services;
- secure data hosting;
- technical support services;
- financial auditing;
- legal advisory services;
- international procurement;
- disaster response operations;
- monitoring and evaluation activities;
- global communications and fundraising campaigns.

International transfers shall occur only where there is a lawful basis and an appropriate organisational purpose.

13.3 Countries to Which Information May Be Transferred

Depending upon operational requirements, personal information may be transferred to countries in which the Foundation or its authorised service providers, donors, or programme partners operate.

Such transfers may involve:

- countries within Africa;
- countries within the European Economic Area (EEA);
- the United Kingdom;
- the United States of America;
- Canada;
- Australia;
- Asian countries where authorised technology providers operate;
- other jurisdictions supporting Foundation programmes or services.

The Foundation does not maintain a fixed list of recipient countries because international partnerships and technology providers may evolve over time.

13.4 International Donors and Development Partners

As an organisation that receives support from international donors and development partners, the Foundation may be required to share limited personal information necessary for:

- grant administration;
- financial accountability;
- donor reporting;
- programme monitoring;
- impact evaluation;
- safeguarding compliance;
- audit requirements;
- project verification;
- regulatory reporting where required by funding agreements.

Only the minimum amount of personal information reasonably necessary for these purposes shall be disclosed.

Where possible, reports shall use aggregated or anonymised information rather than information identifying individual beneficiaries.

13.5 International Cloud Services

To improve operational efficiency, reliability, disaster recovery, and cybersecurity, the Foundation may use reputable cloud-based information technology services that process or store personal information outside the country where it was originally collected.

Examples include secure services supporting:

- email;
- document management;
- cloud storage;
- accounting systems;
- donor management;
- volunteer management;
- website hosting;
- customer relationship management;
- collaboration platforms;
- cybersecurity monitoring;
- encrypted backups;
- business continuity planning.

The Foundation shall select service providers that implement recognised security standards and contractual commitments appropriate to the sensitivity of the information processed.

13.6 Cross-Border Programme Operations

Some Foundation programmes may involve collaboration with organisations located outside the country in which beneficiaries reside.

Examples include:

- regional humanitarian initiatives;
- multinational development projects;
- research collaborations;
- scholarship programmes;
- volunteer exchanges;
- emergency response partnerships;
- environmental conservation initiatives;
- capacity-building programmes.

Where such cooperation requires the sharing of personal information, only information necessary for programme implementation shall be shared.

13.7 Safeguards for International Transfers

Whenever personal information is transferred internationally, Pneuma African Foundation shall implement appropriate safeguards to protect the confidentiality, integrity, and availability of that information.

Such safeguards may include:

- contractual confidentiality obligations;
- data processing agreements where appropriate;
- encryption during transmission;
- encrypted storage;
- access controls;
- role-based permissions;
- authentication mechanisms;
- secure communication channels;
- organisational privacy policies;
- regular security reviews;
- vendor due diligence;
- staff training.

The Foundation shall take reasonable steps to ensure that organisations receiving personal information maintain standards of protection consistent with those required by this Privacy Policy.

13.8 Assessment of International Transfers

Before transferring personal information internationally, the Foundation shall consider factors including:

- the purpose of the transfer;
- the necessity of the transfer;
- the sensitivity of the information;
- the recipient organisation;
- applicable legal requirements;
- available contractual protections;
- technical security measures;
- organisational safeguards;
- potential privacy risks;
- available remedies in the receiving jurisdiction.

Where appropriate, the Foundation may conduct privacy or security assessments before commencing significant international information-sharing arrangements.

13.9 International Service Providers

The Foundation may engage international organisations to provide specialised services including:

- payment processing;
- cybersecurity;
- cloud infrastructure;
- website hosting;
- software support;
- accounting systems;
- communications platforms;
- donor management systems;
- monitoring tools;
- digital collaboration platforms.

Such providers shall process personal information only in accordance with authorised instructions and applicable contractual obligations.

The Foundation shall not knowingly engage service providers whose privacy or security practices present unacceptable risks to the rights of individuals.

13.10 International Transfers During Emergencies

During humanitarian emergencies, disasters, disease outbreaks, or other crises, international transfers of limited personal information may become necessary to facilitate timely humanitarian assistance.

Such transfers may occur for purposes including:

- emergency coordination;
- medical referrals;
- disaster response;
- evacuation support;
- humanitarian logistics;
- safeguarding interventions;
- protection services;
- donor accountability.

Even during emergencies, the Foundation shall seek to ensure that only the minimum amount of personal information necessary is shared and that appropriate safeguards remain in place.

13.11 Rights of Individuals Regarding International Transfers

Individuals whose personal information is processed by the Foundation retain their privacy rights regardless of whether their information is transferred internationally, subject to applicable law.

Where applicable, individuals may:

- request information regarding international transfers affecting their personal information;
- request correction of inaccurate information;
- request deletion where legally permissible;
- object to certain processing activities;
- withdraw consent where consent is the lawful basis for processing;
- submit complaints regarding international transfers.

The exercise of these rights may be subject to legal, contractual, operational, or humanitarian obligations applicable to the Foundation.

13.12 Protection of Sensitive Personal Information During International Transfers

Where sensitive personal information is transferred internationally, the Foundation shall apply enhanced safeguards.

Sensitive information may include:

- health information;
- disability information;
- safeguarding records;
- child protection information;
- financial hardship assessments;
- biometric information where authorised;
- information relating to vulnerable individuals.

Such information shall be shared only where strictly necessary, supported by a lawful basis, and protected through appropriate technical and organisational security measures.

13.13 International Research and Academic Collaboration

The Foundation may participate in international research, educational initiatives, programme evaluations, and academic collaborations.

Where personal information is used for research purposes, the Foundation shall seek, where appropriate, to:

- anonymise information;
- pseudonymise information where anonymisation is not practicable;
- limit access to authorised researchers;
- obtain necessary approvals or consent where required;
- ensure ethical handling of research data.

Research activities shall be conducted in a manner consistent with the Foundation's humanitarian values and respect for the dignity and rights of research participants.

13.14 Continuous Monitoring of International Transfers

International data transfer arrangements shall be reviewed periodically to ensure continued compliance with:

- applicable data protection legislation;
- contractual obligations;

- organisational policies;
- recognised information security standards;
- changes in operational requirements;
- emerging cybersecurity risks.

Where significant changes occur, the Foundation shall review whether additional safeguards or modifications to existing arrangements are necessary.

13.15 Accountability for International Transfers

The Board of Directors, Executive Management, employees, volunteers, consultants, contractors, and authorised representatives of Pneuma African Foundation share responsibility for ensuring that international transfers of personal information are conducted responsibly and lawfully.

The Foundation shall maintain appropriate governance, oversight, and documentation for international transfers and shall investigate any actual or suspected unauthorised international disclosure of personal information.

Any person acting on behalf of the Foundation who knowingly transfers personal information internationally in violation of this Privacy Policy or applicable law may be subject to disciplinary action, termination of contractual relationships, reporting to competent authorities where appropriate, and any other lawful measures necessary to protect affected individuals and the Foundation.

13.16 Commitment to Responsible International Cooperation

Pneuma African Foundation believes that international cooperation is essential to addressing humanitarian challenges and promoting sustainable community development across Africa. The Foundation is equally committed to ensuring that such cooperation is conducted in a manner that respects the privacy, dignity, and rights of every individual whose personal information it processes.

By implementing appropriate safeguards, maintaining transparent governance, and continuously improving its privacy practices, the Foundation seeks to balance effective international collaboration with responsible stewardship of personal information entrusted to its care.

14. DATA SECURITY AND PROTECTION MEASURES

14.1 Introduction

Pneuma African Foundation recognises that the protection of personal information is fundamental to maintaining the trust and confidence of donors, beneficiaries, volunteers, employees, partners, government agencies, and the communities it serves.

The Foundation is committed to implementing and maintaining appropriate administrative, organisational, technical, and physical safeguards designed to protect personal information throughout its lifecycle against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, misuse, theft, corruption, or unauthorised access.

Information security is a shared responsibility. Every Director, employee, volunteer, consultant, contractor, intern, partner, and authorised representative acting on behalf of the Foundation is required to uphold the standards established in this Privacy Policy and the Foundation's broader governance framework.

The Foundation acknowledges that while no information system can guarantee absolute security, it is committed to continually assessing, improving, and strengthening its security controls to minimise risk and respond effectively to evolving cyber threats.

14.2 Security Governance

The Foundation shall establish and maintain an information security governance framework that supports the secure and responsible management of personal information.

This framework shall include:

- governance oversight by the Board of Directors;
- executive responsibility for information security;
- documented policies and procedures;
- defined security roles and responsibilities;
- periodic policy reviews;
- internal compliance monitoring;
- security awareness programmes;
- continuous improvement initiatives.

Information security shall form part of the Foundation's overall risk management and organisational governance processes.

14.3 Security Objectives

The Foundation's security programme seeks to achieve the following objectives:

- protect the confidentiality of personal information;
 - maintain the integrity and accuracy of organisational records;
 - ensure the availability of information when legitimately required;
 - prevent unauthorised access;
 - reduce cybersecurity risks;
 - support humanitarian operations;
 - comply with applicable legal obligations;
 - maintain donor and public confidence;
 - support organisational resilience and business continuity.
-

14.4 Administrative Security Measures

The Foundation shall implement appropriate administrative controls to ensure the responsible handling of personal information.

Administrative safeguards may include:

- privacy and security policies;
 - confidentiality agreements;
 - staff induction programmes;
 - volunteer orientation;
 - periodic security training;
 - acceptable use policies;
 - access approval procedures;
 - segregation of duties;
 - records management procedures;
 - internal audits;
 - disciplinary procedures for policy violations.
-

Every individual authorised to access personal information shall understand their responsibilities regarding confidentiality and information security.

14.5 Technical Security Measures

The Foundation shall implement appropriate technical controls designed to protect electronic information systems.

Such controls may include:

- strong password requirements;
- multi-factor authentication where appropriate;
- encryption during transmission;
- encryption of sensitive stored information where appropriate;
- firewalls;
- intrusion detection and prevention systems;
- malware protection;
- endpoint protection;
- network monitoring;
- secure system configuration;
- vulnerability management;
- software updates;
- security patch management;
- secure remote access;
- secure cloud infrastructure;
- regular backups.

Technical safeguards shall be reviewed periodically to address evolving cybersecurity threats.

14.6 Physical Security Measures

The Foundation shall implement appropriate physical safeguards to protect facilities, equipment, and paper records.

Physical security measures may include:

- controlled building access;
- visitor management procedures;
- secure offices;
- locked filing cabinets;
- restricted archive storage;
- alarm systems where appropriate;
- surveillance systems where lawful;
- secure disposal containers;
- equipment inventory management;
- environmental protections for critical records.

Access to areas containing sensitive information shall be limited to authorised personnel.

14.7 Access Control

Access to personal information shall be granted only to individuals who require such access for legitimate organisational purposes.

Access controls shall include:

- role-based permissions;
- user authentication;
- individual user accounts;
- password management;
- least-privilege principles;
- periodic review of user access rights;
- immediate removal of access following termination of employment or volunteer service where appropriate;
- secure authentication mechanisms.

Users shall not share passwords or authentication credentials with others.

14.8 Confidentiality Obligations

Every person authorised to access personal information on behalf of the Foundation shall be required to maintain confidentiality.

Confidentiality obligations apply to:

- Directors;
- employees;
- volunteers;
- consultants;
- contractors;
- interns;
- researchers;
- programme partners where applicable;
- service providers processing information on behalf of the Foundation.

Confidential information shall not be disclosed except where authorised by this Privacy Policy, required by law, or necessary for legitimate Foundation activities.

Confidentiality obligations shall continue after employment, volunteer service, consultancy engagements, or contractual relationships have ended.

14.9 Encryption

Where appropriate, the Foundation shall use encryption to protect sensitive personal information during storage and transmission.

Encryption may be applied to:

- electronic communications;
- online donation transactions;
- cloud storage;
- backup systems;
- portable storage devices;
- confidential documents transmitted electronically.

Encryption technologies shall be reviewed periodically to ensure continued effectiveness.

14.10 Password and Authentication Security

The Foundation shall implement secure authentication practices designed to reduce the risk of unauthorised access.

Users shall be expected to:

- create strong passwords;
- protect authentication credentials;
- avoid password sharing;
- change compromised passwords immediately;
- use multi-factor authentication where available;
- report suspected credential compromise without delay.

System administrators shall implement appropriate authentication controls consistent with recognised security standards.

14.11 Device Security

Devices used to access Foundation information shall be protected through appropriate security measures.

These may include:

- device passwords;
- encryption;
- automatic locking;
- antivirus protection;
- secure operating systems;
- software updates;
- remote wipe capabilities where appropriate;
- secure mobile device management.

Where personal devices are authorised for Foundation business, they shall comply with applicable organisational security requirements.

14.12 Network Security

The Foundation shall maintain appropriate network security measures to reduce cybersecurity risks.

Network protections may include:

- secure network architecture;
- firewall protection;
- secure wireless networks;
- network segmentation where appropriate;
- intrusion monitoring;
- secure remote access;
- virtual private networks (VPNs) where appropriate;
- traffic monitoring;
- denial-of-service protection where feasible.

Security logs may be maintained to assist with threat detection and incident investigations.

14.13 Secure Development and Website Security

Where the Foundation develops or operates digital platforms, reasonable steps shall be taken to ensure that security is incorporated throughout the development and maintenance lifecycle.

Security practices may include:

- secure coding standards;
- application testing;
- vulnerability assessments;
- penetration testing where appropriate;
- software updates;
- dependency management;
- code review procedures;
- secure hosting environments.

The Foundation's website shall be monitored to protect against unauthorised access, malware, malicious code, and other cybersecurity threats.

14.14 Records Management and Secure Storage

Personal information shall be stored in a manner that protects confidentiality, integrity, and availability.

Storage practices may include:

- secure electronic databases;
- encrypted cloud storage where appropriate;
- secure physical archives;
- controlled access storage facilities;
- records retention schedules;
- regular backups;
- disaster recovery arrangements.

Only authorised personnel shall have access to stored personal information.

14.15 Secure Disposal of Personal Information

When personal information is no longer required and legal or operational retention periods have expired, the Foundation shall securely dispose of such information.

Secure disposal methods may include:

- secure deletion of electronic records;
- physical destruction of storage media where appropriate;
- shredding confidential paper records;
- certified disposal services;
- permanent removal from backup systems where practicable and appropriate.

The Foundation shall take reasonable steps to ensure that disposed information cannot be reconstructed or recovered by unauthorised persons.

14.16 Monitoring and Security Audits

The Foundation may conduct periodic monitoring and security assessments to evaluate the effectiveness of its information security programme.

These activities may include:

- internal security reviews;
- vulnerability assessments;
- risk assessments;
- compliance audits;
- system monitoring;
- penetration testing where appropriate;
- review of access logs;
- policy compliance reviews.

Monitoring activities shall be conducted lawfully and proportionately while respecting the privacy rights of individuals.

14.17 Security Incident Management

Despite the implementation of appropriate safeguards, security incidents may occur.

Examples include:

- unauthorised access;
- malware infections;
- phishing attacks;
- accidental disclosure;
- lost devices;
- theft of equipment;
- ransomware attacks;
- system failures;
- human error.

The Foundation shall maintain procedures for:

- identifying security incidents;
 - containing threats;
 - investigating incidents;
 - mitigating harm;
 - restoring affected systems;
 - documenting incidents;
 - implementing corrective actions;
 - notifying affected individuals and competent authorities where required by applicable law.
-

14.18 Business Continuity and Disaster Recovery

The Foundation recognises the importance of maintaining the availability of critical information during emergencies.

Accordingly, the Foundation shall implement reasonable business continuity and disaster recovery measures, which may include:

- secure data backups;
- redundant storage where appropriate;
- disaster recovery procedures;
- emergency communications;
- continuity planning for critical systems;
- periodic testing of recovery capabilities.

These measures support the Foundation's ability to continue delivering humanitarian and development programmes during disruptive events.

14.19 Security Awareness and Training

Information security depends upon informed and responsible personnel.

Accordingly, the Foundation shall provide appropriate security awareness training for Directors, employees, volunteers, consultants, and contractors.

Training may address:

- privacy responsibilities;
- phishing awareness;
- password security;
- safeguarding confidential information;
- secure use of information technology;
- recognising security incidents;
- reporting security concerns;
- responsible handling of beneficiary and donor information.

Training programmes shall be reviewed periodically to reflect emerging risks and technological developments.

14.20 Responsibilities of Individuals

Every individual who has access to Foundation information is responsible for:

- protecting confidential information;
- complying with this Privacy Policy;
- following organisational security procedures;

- reporting suspected security incidents immediately;
- using Foundation systems responsibly;
- preventing unauthorised disclosure of information;
- protecting passwords and authentication credentials;
- safeguarding physical and electronic records.

Failure to comply with these responsibilities may result in disciplinary action, termination of employment or contractual relationships, or other lawful measures.

14.21 Continuous Improvement

Cybersecurity threats, technology, and legal requirements continue to evolve.

The Foundation is committed to regularly reviewing and improving its information security programme through:

- periodic policy reviews;
- technological improvements;
- security risk assessments;
- independent audits where appropriate;
- lessons learned from incidents;
- staff feedback;
- evolving best practices.

Continuous improvement is essential to maintaining the confidence of donors, beneficiaries, volunteers, employees, partners, and the communities served by the Foundation.

14.22 Commitment to Information Security

Pneuma African Foundation considers information security to be an integral part of good governance, ethical stewardship, and humanitarian service.

The Foundation shall continue to invest in appropriate organisational, technical, physical, and administrative safeguards to ensure that personal information remains protected throughout its lifecycle.

By maintaining a comprehensive information security framework, the Foundation seeks to uphold the privacy, dignity, and trust of every individual who interacts with its programmes, services, website, and operations.

15. DATA RETENTION AND SECURE DISPOSAL

15.1 Introduction

Pneuma African Foundation recognises that responsible management of personal information extends beyond its collection and use to include the appropriate retention and secure disposal of such information.

The Foundation is committed to retaining personal information only for as long as it is reasonably necessary to fulfil the purposes for which it was collected, to comply with applicable legal and regulatory obligations, to support legitimate organisational interests, and to preserve records of enduring historical or governance value.

Once the applicable retention period has expired and there is no continuing lawful basis for retaining the information, the Foundation shall ensure that such information is securely deleted, anonymised, or destroyed in a manner that prevents unauthorised access, reconstruction, or misuse.

This Section establishes the Foundation's principles and procedures for the retention, archival, and secure disposal of personal information throughout its lifecycle.

15.2 Purpose of Data Retention

The Foundation retains personal information for legitimate organisational purposes, including:

- delivering humanitarian and development programmes;
- administering donations and grants;
- maintaining financial accountability;
- fulfilling contractual obligations;
- complying with legal and regulatory requirements;
- protecting the rights of beneficiaries, donors, volunteers, employees, and partners;
- responding to audits and inspections;
- supporting safeguarding obligations;
- preserving governance records;
- maintaining organisational continuity;
- resolving disputes;
- defending legal claims;
- supporting institutional learning and historical records.

The Foundation shall not retain personal information indefinitely unless there is a lawful and justifiable reason for doing so.

15.3 Retention Principles

The Foundation shall manage the retention of personal information in accordance with the following principles:

(a) Lawfulness

Information shall be retained only where permitted or required by applicable law.

(b) Purpose Limitation

Information shall not be retained once the purpose for which it was collected has been fulfilled unless another lawful basis for retention exists.

(c) Data Minimisation

Only information reasonably necessary for legitimate organisational purposes shall be retained.

(d) Accuracy

Retained records shall, where reasonably practicable, be kept accurate, complete, and up to date.

(e) Security

Retained information shall remain subject to appropriate technical, physical, and organisational safeguards throughout the retention period.

(f) Accountability

The Foundation shall maintain appropriate oversight and governance over retained information.

15.4 Categories of Information Subject to Retention

The Foundation may retain records relating to:

- donors;
- beneficiaries;
- volunteers;
- employees;
- consultants;
- contractors;
- suppliers;
- grant applicants;

- programme participants;
- community assessments;
- safeguarding matters;
- financial transactions;
- governance records;
- legal matters;
- procurement;
- audits;
- monitoring and evaluation;
- website administration;
- communications;
- complaints;
- incident reports.

Each category shall be retained for a period appropriate to its purpose and applicable legal requirements.

15.5 Standard Retention Periods

Retention periods may vary depending upon the nature of the information, applicable law, contractual obligations, donor requirements, safeguarding considerations, and organisational needs.

The following table provides the Foundation's general retention framework.

Record Category	Standard Retention Period
Website enquiries	Up to 2 years after resolution
Newsletter subscriptions	Until the individual unsubscribes or consent is withdrawn
General correspondence	Up to 5 years
Donor records	Up to 7 years after the last financial transaction, unless a longer period is required by law
Financial records	At least 7 years, or longer where required by law
Grant administration records	Up to 10 years after project closure, subject to donor agreements
Procurement records	Up to 7 years after contract completion
Volunteer records	Up to 7 years after volunteer service ends
Employment records	As required by applicable employment and tax laws, and generally not less than 7 years after employment ends
Safeguarding records	Retained for periods appropriate to safeguarding responsibilities and applicable legal requirements, which may be significantly longer than general administrative records
Child protection records	Retained for periods consistent with safeguarding obligations and applicable law

Record Category	Standard Retention Period
Programme monitoring and evaluation records	Up to 10 years after programme completion where appropriate
Audit records	Up to 10 years
Governance records (Board minutes, resolutions, constitutional documents)	May be retained permanently as part of the Foundation's official corporate records
Legal proceedings	Until final resolution of the matter and expiry of any applicable limitation periods

These retention periods represent general guidance. Specific legal obligations, grant agreements, or regulatory requirements may require longer retention.

15.6 Factors Considered When Determining Retention Periods

When determining appropriate retention periods, the Foundation shall consider:

- applicable laws and regulations;
- contractual obligations;
- donor requirements;
- safeguarding responsibilities;
- audit requirements;
- taxation obligations;
- financial accountability;
- operational necessity;
- public interest;
- historical significance;
- organisational governance;
- ongoing legal proceedings;
- the sensitivity of the information;
- the potential impact on individuals if retained or destroyed.

15.7 Archival Records

Certain records possess enduring legal, governance, historical, or institutional value and may therefore be retained permanently or for extended periods.

Examples include:

- constitutional documents;
- certificates of incorporation or registration;

- Board minutes;
- annual reports;
- strategic plans;
- audited financial statements;
- significant policy documents;
- major partnership agreements;
- historical publications;
- organisational photographs of historical significance;
- records documenting the Foundation's establishment and development.

Where personal information forms part of archival records, the Foundation shall continue to protect such information through appropriate access controls and confidentiality measures.

15.8 Suspension of Disposal (Legal Hold)

Where the Foundation becomes aware of:

- actual or anticipated litigation;
- regulatory investigations;
- law enforcement investigations;
- audits;
- safeguarding investigations;
- employment disputes;
- contractual disputes; or
- other legal proceedings,

the Foundation may suspend the routine destruction of relevant records.

Such records shall be preserved until the matter has been fully resolved and any applicable legal obligations to retain the information have ended.

15.9 Secure Storage During the Retention Period

While personal information is retained, the Foundation shall ensure that appropriate safeguards remain in place.

These safeguards may include:

- encrypted electronic storage where appropriate;
- secure cloud infrastructure;
- restricted physical archives;
- role-based access controls;

- password protection;
- secure backup systems;
- environmental protection for physical records;
- confidentiality obligations for authorised personnel.

The level of protection shall be proportionate to the sensitivity of the information being retained.

15.10 Secure Disposal of Electronic Information

When electronic records reach the end of their retention period, the Foundation shall dispose of them securely.

Secure disposal methods may include:

- permanent deletion from active systems;
- secure erasure of storage media;
- cryptographic erasure where appropriate;
- overwriting of electronic media;
- secure destruction of removable storage devices;
- deletion from cloud services in accordance with contractual arrangements;
- destruction of obsolete backup media where appropriate.

The Foundation shall take reasonable steps to ensure that deleted information cannot be readily recovered or reconstructed by unauthorised persons.

15.11 Secure Disposal of Physical Records

Paper records containing personal information shall be destroyed using secure methods.

These methods may include:

- cross-cut shredding;
- pulping;
- incineration where lawful and appropriate;
- secure destruction by authorised document destruction providers.

Physical records shall not be discarded in ordinary waste where they contain confidential or personal information.

15.12 Disposal of Information Held by Third Parties

Where personal information has been processed on behalf of the Foundation by authorised service providers, the Foundation shall, where appropriate, require those providers to:

- return personal information upon completion of services;
- securely delete information no longer required;
- certify destruction where contractually required;
- comply with applicable contractual and legal obligations regarding disposal.

The Foundation shall take reasonable steps to verify that third parties fulfil their contractual responsibilities concerning information disposal.

15.13 Anonymisation and Pseudonymisation

Where continued use of information is desirable for research, statistical analysis, programme evaluation, or historical reporting, the Foundation may anonymise or pseudonymise personal information where appropriate.

Anonymised information that can no longer reasonably identify an individual may be retained for longer periods for legitimate organisational purposes, including impact measurement and institutional learning.

15.14 Individual Requests for Deletion

Where individuals exercise their rights to request the deletion of personal information, the Foundation shall consider such requests in accordance with:

- applicable law;
- contractual obligations;
- safeguarding responsibilities;
- legal retention requirements;
- financial record-keeping obligations;
- the legitimate interests of the Foundation.

The Foundation may decline a deletion request where retention is required or permitted by law, necessary for the establishment, exercise, or defence of legal claims, or essential to safeguarding, audit, or governance obligations. The reasons for any refusal shall be communicated to the individual where required by applicable law.

15.15 Documentation of Disposal Activities

The Foundation may maintain records of significant disposal activities for accountability and audit purposes.

Such records may include:

- the categories of records destroyed;
- the date of destruction;
- the method of destruction;
- the individual or service provider responsible for the destruction;
- any relevant authorisations.

These records support the Foundation's governance and demonstrate compliance with this Privacy Policy.

15.16 Responsibilities for Records Retention

The Board of Directors shall provide oversight of the Foundation's records management and retention framework.

Executive Management shall ensure that appropriate procedures, systems, and resources are in place to implement this Policy.

Employees, volunteers, consultants, contractors, and other authorised representatives shall:

- retain information only as required;
- protect retained records from unauthorised access;
- comply with approved retention schedules;
- report concerns regarding improper retention or disposal;
- participate in relevant records management training.

Failure to comply with these responsibilities may result in disciplinary action or other appropriate measures.

15.17 Periodic Review of Retained Information

The Foundation shall periodically review retained records to determine whether:

- the information remains necessary;
- retention periods have expired;
- records should be archived;
- information should be securely destroyed;
- legal holds remain in effect;
- additional security measures are required.

These reviews help ensure that personal information is not retained longer than necessary and that records management remains aligned with legal requirements and organisational needs.

15.18 Commitment to Responsible Records Management

Pneuma African Foundation recognises that responsible records management is an essential component of good governance, transparency, accountability, and public trust.

By implementing structured retention schedules, maintaining secure storage, preserving records of enduring value, and ensuring the secure disposal of information that is no longer required, the Foundation seeks to balance its operational, legal, and historical responsibilities with its commitment to protecting the privacy and dignity of every individual whose personal information it processes.

16. YOUR PRIVACY RIGHTS

16.1 Introduction

Pneuma African Foundation recognises that every individual has important rights concerning their personal information. Respecting these rights is fundamental to the Foundation's commitment to transparency, accountability, human dignity, and responsible stewardship.

The Foundation is committed to ensuring that individuals are informed of their privacy rights and are provided with reasonable opportunities to exercise those rights in accordance with applicable data protection laws, this Privacy Policy, and the Foundation's legitimate operational, legal, safeguarding, and humanitarian obligations.

The exercise of these rights may be subject to certain legal limitations where the Foundation is required or permitted by law to retain or continue processing personal information.

16.2 Our Commitment to Individual Rights

The Foundation is committed to ensuring that individuals can:

- understand how their personal information is processed;
- access information held about them;
- request correction of inaccurate information;
- request deletion of personal information where appropriate;
- object to certain processing activities;
- request restrictions on processing in appropriate circumstances;
- withdraw consent where consent is the legal basis for processing;
- lodge complaints regarding privacy matters;
- receive fair and timely responses to privacy-related requests.

The Foundation shall handle all requests respectfully, fairly, and without discrimination.

16.3 Right to Be Informed

Individuals have the right to receive clear and understandable information regarding:

- what personal information the Foundation collects;
- why the information is collected;
- how the information is used;
- who may receive the information;
- how long information is retained;
- applicable security measures;
- available privacy rights;
- how to contact the Foundation regarding privacy concerns.

This Privacy Policy serves as one of the Foundation's primary privacy notices.

Where additional information is necessary for specific programmes or services, supplementary privacy notices may also be provided.

16.4 Right of Access

Individuals may request confirmation as to whether the Foundation processes personal information relating to them.

Subject to applicable law and verification of identity, individuals may request access to:

- the categories of personal information held;
- the purposes for which the information is processed;
- the sources from which the information was obtained;
- categories of recipients with whom the information has been shared;
- applicable retention periods;

- available privacy rights.

Where legally permissible, the Foundation shall provide access within a reasonable period after receiving a valid request.

The Foundation may request sufficient information to verify the identity of the individual before disclosing personal information.

16.5 Right to Correction (Rectification)

Individuals have the right to request correction of personal information that is:

- inaccurate;
- incomplete;
- outdated;
- misleading.

Where appropriate, the Foundation shall:

- correct inaccurate information;
- update incomplete records;
- amend incorrect contact details;
- verify disputed information before making changes.

The Foundation may request supporting documentation where necessary to verify the requested correction.

16.6 Right to Request Deletion (Erasure)

Individuals may request that the Foundation delete personal information concerning them where:

- the information is no longer necessary for the purpose for which it was collected;
- consent has been withdrawn and no other lawful basis exists;
- the information has been processed unlawfully;
- deletion is required by applicable law.

However, the Foundation may decline deletion requests where retention remains necessary for:

- compliance with legal obligations;
- safeguarding responsibilities;
- financial record-keeping;
- fraud prevention;

- ongoing contractual obligations;
- legal claims;
- audit requirements;
- public interest obligations;
- historical or archival purposes where permitted by law.

Where deletion is not possible, the Foundation shall explain the lawful basis for retaining the information, unless prohibited by law.

16.7 Right to Restrict Processing

Individuals may request that the Foundation temporarily restrict the processing of their personal information in certain circumstances, including where:

- the accuracy of information is being verified;
- processing is alleged to be unlawful;
- deletion is not desired;
- the Foundation no longer requires the information but the individual requires it for legal claims;
- an objection to processing is under consideration.

Where processing is restricted, the Foundation shall continue to protect the information but shall limit further processing except where permitted by law.

16.8 Right to Object to Processing

Where permitted by applicable law, individuals may object to the processing of their personal information where processing is based upon the Foundation's legitimate interests or public interest functions.

The Foundation shall carefully consider each objection.

Processing may continue where:

- compelling legitimate grounds exist;
 - legal obligations require continued processing;
 - safeguarding responsibilities require continued processing;
 - processing is necessary for legal claims;
 - the Foundation's humanitarian responsibilities outweigh the grounds for objection in accordance with applicable law.
-

16.9 Right to Withdraw Consent

Where the Foundation relies upon an individual's consent as the lawful basis for processing personal information, that consent may be withdrawn at any time.

Withdrawal of consent shall not affect:

- processing undertaken before consent was withdrawn;
- processing based upon another lawful basis;
- legal obligations requiring continued retention;
- safeguarding responsibilities;
- financial accountability obligations.

Requests to withdraw consent may be submitted using the contact information provided in this Privacy Policy.

16.10 Right to Data Portability

Where applicable under relevant law and where technically feasible, individuals may request that personal information they have provided to the Foundation be supplied:

- in a commonly used electronic format; or
- directly to another organisation where technically practicable and legally permissible.

This right applies only where:

- processing is based upon consent or contractual necessity; and
- processing is carried out by automated means.

The Foundation may decline portability requests where applicable legal exceptions apply.

16.11 Rights Relating to Marketing Communications

Individuals may choose whether to receive non-essential communications from the Foundation.

Where individuals no longer wish to receive newsletters, fundraising updates, event invitations, or other promotional communications, they may:

- unsubscribe using the link provided in electronic communications;
- contact the Foundation directly;

- update their communication preferences where available.

Certain essential communications may continue where necessary to administer donations, volunteer activities, programme participation, contractual relationships, or legal obligations.

16.12 Rights Regarding Automated Decision-Making

The Foundation does not ordinarily make decisions that produce legal or similarly significant effects solely through automated processing without meaningful human involvement.

Should the Foundation introduce such processing in the future, appropriate safeguards shall be implemented in accordance with applicable law, including providing affected individuals with information about the processing and, where required, opportunities for human review.

16.13 Rights of Children and Parents or Legal Guardians

Where the Foundation processes personal information relating to children, parents or lawful guardians may exercise privacy rights on behalf of the child where permitted by applicable law.

In exercising these rights, the Foundation shall always consider:

- the best interests of the child;
- safeguarding obligations;
- legal requirements;
- the child's evolving capacity and rights under applicable law.

The Foundation shall not disclose information where doing so could place a child or vulnerable individual at risk.

16.14 Exercising Your Privacy Rights

Individuals wishing to exercise any privacy rights under this Policy may submit a request by contacting the Foundation using the contact details provided in **Section 24 – Contact Information**.

Requests should, where possible, include:

- the individual's full name;
- sufficient information to identify the relevant records;
- contact details;
- a clear description of the request;
- supporting documentation where appropriate.

The Foundation may request additional information to verify identity before processing a request.

16.15 Identity Verification

To protect personal information from unauthorised disclosure, the Foundation may require reasonable verification of identity before:

- providing access to personal information;
- correcting records;
- deleting information;
- restricting processing;
- disclosing confidential records.

Verification procedures shall be proportionate to the sensitivity of the information requested.

16.16 Response Time

The Foundation shall acknowledge privacy requests promptly and endeavour to respond within a reasonable period, taking into account:

- the complexity of the request;
- the volume of information involved;
- applicable legal requirements;
- operational circumstances.

Where additional time is reasonably required, the Foundation shall, where appropriate, inform the individual of the reason for the delay and the expected timeframe for a response.

16.17 Circumstances Where Requests May Be Refused

The Foundation may refuse or limit a request where permitted by applicable law, including where:

- disclosure would adversely affect the rights of another individual;
- information is subject to legal privilege;
- disclosure would prejudice an investigation;
- retention is required by law;
- safeguarding obligations require confidentiality;
- disclosure would compromise security measures;
- the request is manifestly unfounded, repetitive, or excessive.

Where a request is refused, the Foundation shall provide reasons where required by law and, where appropriate, information about available avenues for review or complaint.

16.18 Right to Lodge a Complaint

Individuals who believe that the Foundation has not handled their personal information appropriately are encouraged to contact the Foundation so that concerns may be addressed promptly and fairly.

If an individual remains dissatisfied after the Foundation has considered the matter, they may have the right to submit a complaint to the relevant regulatory or supervisory authority responsible for privacy and data protection in the applicable jurisdiction.

The Foundation shall cooperate with competent authorities in accordance with applicable law.

16.19 No Retaliation

The Foundation shall not discriminate against, penalise, or retaliate against any individual for exercising privacy rights in good faith.

No person shall be denied access to humanitarian assistance, volunteer opportunities, employment consideration, or other legitimate Foundation services solely because they have exercised rights available under this Privacy Policy, except where the exercise of those rights makes it impossible to provide a requested service or where continued processing is legally or operationally necessary.

16.20 Commitment to Respecting Privacy Rights

Pneuma African Foundation believes that respecting privacy rights is an essential expression of accountability, integrity, and respect for human dignity.

The Foundation is committed to fostering a culture in which privacy rights are understood, protected, and respected across all programmes, partnerships, digital platforms, and organisational activities. Through transparent procedures, responsive communication, and responsible governance, the Foundation seeks to ensure that every individual is treated fairly and that their personal information is handled with the care and respect it deserves.

17. COOKIES, TRACKING TECHNOLOGIES, AND WEBSITE ANALYTICS

17.1 Introduction

Pneuma African Foundation uses cookies and similar technologies to ensure the effective operation, security, performance, and accessibility of its website and digital services.

These technologies help the Foundation provide a reliable and user-friendly online experience, understand how visitors interact with the website, improve digital services, protect against cyber threats, and support the Foundation's humanitarian, educational, and fundraising activities.

The Foundation is committed to using cookies and tracking technologies responsibly, transparently, and in accordance with applicable privacy and data protection laws.

This section should be read together with the Foundation's separate **Cookie Policy**, which provides more detailed information regarding the specific categories of cookies used on the website.

17.2 What Are Cookies?

Cookies are small text files placed on a user's computer, mobile phone, tablet, or other internet-enabled device when visiting a website.

Cookies enable websites to:

- recognise returning visitors;
- remember user preferences;
- improve website functionality;
- enhance website security;
- analyse website performance;
- support accessibility features;
- facilitate secure online transactions;
- improve the overall user experience.

Cookies do not generally damage a user's device or provide unauthorised access to files stored on that device.

17.3 Other Tracking Technologies

In addition to cookies, the Foundation's website may use other technologies that perform similar functions.

These may include:

- web beacons;
- tracking pixels;
- local storage technologies;
- session identifiers;
- server log files;
- analytics tags;
- application programming interface (API) event tracking;
- security monitoring tools.

These technologies assist the Foundation in maintaining secure, efficient, and effective digital services.

17.4 Purposes for Which Cookies Are Used

The Foundation may use cookies and similar technologies for purposes including:

- maintaining website functionality;
- remembering user preferences;
- supporting accessibility settings;
- improving website navigation;
- enhancing website performance;
- protecting against malicious activity;
- detecting fraud;
- securing online donation processes;
- analysing visitor behaviour;
- measuring website traffic;
- improving content;
- understanding user engagement;
- troubleshooting technical issues;
- supporting digital communications;
- maintaining session security.

Cookies are not used to undermine users' privacy or to engage in unlawful tracking.

17.5 Categories of Cookies Used

The Foundation may use the following categories of cookies.

A. Strictly Necessary Cookies

These cookies are essential for the operation of the website.

Without these cookies, certain website functions may not operate correctly.

Examples include cookies used for:

- website security;
- user authentication;
- session management;
- load balancing;
- fraud prevention;
- accessibility functionality;
- online donation processing;
- form submissions.

Because these cookies are essential to the operation of the website, they generally cannot be disabled through the Foundation's cookie preference system.

B. Functional Cookies

Functional cookies improve the user experience by remembering choices made by visitors.

These cookies may remember:

- preferred language;
- region;
- accessibility settings;
- font preferences where available;
- previously selected website options;
- login preferences where appropriate.

Functional cookies help personalise the website without identifying users unnecessarily.

C. Performance and Analytics Cookies

Performance cookies help the Foundation understand how visitors use the website.

Information collected may include:

- pages visited;
- time spent on pages;
- navigation paths;
- device types;
- browser types;
- website performance;
- referral sources;
- search terms used on the website;
- download statistics;
- user engagement.

Where practical, this information shall be aggregated or anonymised.

Analytics information helps the Foundation:

- improve website design;
- improve accessibility;
- identify technical issues;
- enhance user experience;
- evaluate digital communications;
- improve educational resources.

D. Security Cookies

Security-related cookies may be used to:

- detect suspicious activity;
- prevent unauthorised access;
- reduce cybersecurity risks;
- protect user accounts;
- prevent automated attacks;
- detect malicious software;
- secure donation transactions.

Security cookies form an important part of the Foundation's cybersecurity framework.

E. Third-Party Cookies

Some pages of the Foundation's website may include services provided by trusted third parties.

Examples may include:

- secure payment providers;
- mapping services;
- embedded videos;
- social media integrations;
- accessibility tools;
- website analytics providers.

These third-party services may place cookies on users' devices in accordance with their own privacy policies.

The Foundation does not control third-party cookie practices and encourages users to review the privacy policies of those providers where appropriate.

17.6 Website Analytics

The Foundation may use website analytics services to understand how visitors interact with the website.

Analytics information may include:

- number of visitors;
- pages viewed;
- referral websites;
- navigation behaviour;
- session duration;
- geographical region (general, not precise location);
- browser type;
- operating system;
- device type;
- website performance data.

Analytics information helps the Foundation:

- improve website usability;
- optimise website performance;
- improve programme information;
- evaluate public awareness campaigns;
- enhance donor engagement;
- improve volunteer recruitment;
- support strategic planning.

Where reasonably practicable, analytics information shall be processed in aggregated or anonymised form.

17.7 Online Donations

Where users make donations through the Foundation's website, cookies or related technologies may be used to:

- maintain secure donation sessions;
- prevent duplicate submissions;
- detect fraudulent activity;
- protect payment transactions;
- confirm successful processing;
- improve transaction reliability.

Payment card information is processed through authorised payment service providers and not through cookies themselves.

17.8 Website Security Monitoring

The Foundation continuously monitors its website to protect visitors and organisational systems from cybersecurity threats.

Security monitoring technologies may assist in detecting:

- malicious software;
- automated attacks;
- denial-of-service attacks;
- unauthorised login attempts;
- suspicious browsing activity;
- fraudulent transactions;
- attempts to compromise website security.

Such monitoring is conducted solely for legitimate security purposes.

17.9 Social Media and Embedded Content

The Foundation's website may include links to or embedded content from third-party platforms.

Examples include:

- videos;
- social media feeds;
- maps;
- online forms;

- fundraising platforms.

Where users interact with such content, the third-party provider may collect information in accordance with its own privacy practices.

The Foundation encourages users to review the privacy policies of any third-party platforms they choose to access.

17.10 Managing Cookie Preferences

Where technically feasible, visitors shall be provided with the opportunity to manage their cookie preferences through the Foundation's website.

Depending on the technology used, visitors may be able to:

- accept all cookies;
- reject non-essential cookies;
- customise cookie preferences;
- withdraw previously granted consent;
- modify cookie settings at any time.

Changes to cookie preferences may affect certain website functionality.

17.11 Browser Controls

Most internet browsers allow users to control cookies through browser settings.

Users may generally choose to:

- block cookies;
- delete existing cookies;
- receive notifications before cookies are stored;
- restrict third-party cookies;
- clear browsing data.

Instructions for managing cookies can usually be found within the help documentation of the user's browser.

Disabling certain cookies may affect the operation of some features of the Foundation's website.

17.12 Do Not Track Signals

Some web browsers provide "Do Not Track" ("DNT") settings intended to communicate a user's preference regarding online tracking.

Because there is currently no universally accepted standard governing how websites should respond to DNT signals, the Foundation may not respond to all such signals in a consistent manner.

The Foundation will continue to monitor developments in this area and review its practices as industry standards evolve.

17.13 Children's Privacy and Cookies

The Foundation does not knowingly use cookies or tracking technologies to profile children for advertising or commercial marketing purposes.

Where Foundation programmes involve children, any use of digital technologies shall be consistent with the Foundation's safeguarding responsibilities and commitment to protecting children's privacy.

17.14 Data Protection and Security

Information collected through cookies and similar technologies shall be protected using appropriate technical and organisational security measures.

The Foundation shall:

- limit access to authorised personnel;
- use secure storage systems;
- protect analytics information;
- review technology providers periodically;
- implement appropriate cybersecurity safeguards.

Information collected through cookies shall not be retained longer than necessary for the purposes described in this Privacy Policy.

17.15 Changes to Cookie Technologies

As the Foundation develops new digital services or adopts improved technologies, the cookies and tracking technologies used on the website may change.

Where significant changes affect users' privacy, the Foundation shall update this Privacy Policy and, where required by applicable law, obtain any necessary consent before implementing new non-essential cookies.

The Foundation encourages users to review this Privacy Policy and the Cookie Policy periodically to remain informed about current practices.

17.16 Commitment to Responsible Use of Digital Technologies

Pneuma African Foundation is committed to ensuring that cookies, tracking technologies, and website analytics are used responsibly, transparently, and only for legitimate organisational purposes.

The Foundation does not use these technologies to sell personal information, conduct unlawful surveillance, or engage in intrusive commercial profiling. Instead, they are used to support secure website operations, improve user experience, strengthen digital services, enhance accessibility, protect against cyber threats, and advance the Foundation's humanitarian mission.

By maintaining responsible digital practices and respecting user choices, the Foundation seeks to provide a secure and trustworthy online environment for donors, beneficiaries, volunteers, partners, and members of the public.

18. THIRD-PARTY WEBSITES, EXTERNAL LINKS, AND ONLINE SERVICES

18.1 Introduction

Pneuma African Foundation's website may contain links to third-party websites, online platforms, digital services, social media channels, payment gateways, cloud-based applications, and other external resources that are not owned, operated, or controlled by the Foundation.

These external resources are provided for the convenience of visitors, to facilitate programme delivery, fundraising, volunteer engagement, educational activities, partnerships, and access to additional information.

While the Foundation seeks to engage only reputable organisations and service providers, it cannot guarantee or assume responsibility for the privacy, security, accessibility, availability, or content of third-party websites or services.

Users who access third-party services do so subject to the terms, privacy policies, and practices of those respective organisations.

18.2 External Website Links

The Foundation's website may include links to external websites for purposes such as:

- humanitarian partnerships;
- donor organisations;
- government agencies;
- educational institutions;
- research organisations;
- community resources;
- funding opportunities;
- volunteer registration;
- event management;
- professional service providers;
- public awareness campaigns.

The inclusion of a link does not constitute an endorsement of the views, products, services, policies, or content of the linked organisation unless expressly stated by the Foundation.

18.3 Third-Party Online Services

The Foundation may utilise trusted third-party online services to support its operations.

These services may include:

- online donation platforms;
- payment gateways;
- cloud storage providers;
- email communication services;
- customer relationship management (CRM) systems;
- volunteer management systems;
- grant management platforms;
- webinar and virtual meeting platforms;
- document collaboration services;
- accounting software;
- website hosting services;
- cybersecurity services;

- website analytics providers;
- digital communication platforms.

Such providers may process personal information on behalf of the Foundation in accordance with contractual obligations and applicable data protection laws.

18.4 Payment Service Providers

To facilitate secure online donations and other authorised financial transactions, the Foundation may engage recognised third-party payment processors.

These providers may process information including:

- payer identification details;
- billing information;
- transaction reference numbers;
- payment confirmations;
- fraud prevention information;
- transaction security data.

The Foundation does not store complete payment card details on its own systems unless expressly required for lawful operational purposes and protected through appropriate security measures.

Payment processing is governed by the privacy and security practices of the relevant payment provider.

18.5 Social Media Platforms

The Foundation maintains official accounts on various social media platforms to engage with donors, beneficiaries, volunteers, partners, and the wider public.

Interactions with the Foundation through social media platforms are also governed by the privacy policies and terms of use of those respective platforms.

Information voluntarily shared by users through comments, messages, reactions, or public posts may become visible to other users depending upon the privacy settings of the platform.

Users are encouraged to exercise discretion when sharing personal or sensitive information through social media.

18.6 Embedded Content

The Foundation's website may include embedded content from authorised third-party providers.

Examples may include:

- educational videos;
- interactive maps;
- multimedia presentations;
- online forms;
- event registration tools;
- livestreams;
- publications;
- fundraising widgets.

Embedded content may function as though the visitor has accessed the third-party website directly.

Accordingly, the third-party provider may collect information in accordance with its own privacy policy.

18.7 Third-Party Applications

The Foundation may provide access to or integrate with authorised third-party applications supporting:

- volunteer management;
- donor engagement;
- programme registration;
- learning management;
- surveys;
- impact assessments;
- newsletters;
- online training;
- digital collaboration;
- customer support.

Such applications may require users to create separate accounts or accept additional terms established by the third-party provider.

The Foundation encourages users to review those terms before using such services.

18.8 Information Shared with Third Parties

Where personal information is shared with authorised third-party service providers, the Foundation shall seek to ensure that:

- the sharing is lawful;
- only the minimum necessary information is disclosed;
- appropriate contractual protections are in place;
- confidentiality obligations apply;
- reasonable security measures are maintained;
- the information is used only for authorised purposes.

Third-party providers shall not be authorised to use personal information for their own unrelated commercial purposes except where the individual has chosen to interact directly with that provider under its own terms.

18.9 Third-Party Privacy Policies

Each third-party organisation maintains its own privacy practices.

Accordingly, users are encouraged to review the privacy policies of external organisations before:

- making online donations through third-party platforms;
- registering for external events;
- creating user accounts;
- downloading applications;
- subscribing to third-party services;
- participating in external surveys;
- accessing embedded content.

The Foundation is not responsible for changes made by third parties to their privacy policies after links have been published on the Foundation's website.

18.10 Third-Party Security

Although the Foundation undertakes reasonable due diligence when selecting service providers, it cannot guarantee the security of systems operated by independent organisations.

The Foundation shall make reasonable efforts to work with providers that demonstrate appropriate standards of:

- cybersecurity;

- privacy protection;
- confidentiality;
- regulatory compliance;
- operational reliability;
- information security.

Users acknowledge that no third-party online service can guarantee absolute security.

18.11 Availability of External Services

The Foundation does not guarantee the continuous availability of third-party websites or online services.

External services may become unavailable due to:

- maintenance;
- technical failures;
- internet disruptions;
- cybersecurity incidents;
- service provider decisions;
- legal restrictions;
- operational changes.

The Foundation shall not be liable for interruptions or failures affecting services beyond its reasonable control.

18.12 External Content

The Foundation is not responsible for:

- the accuracy of information published on third-party websites;
- opinions expressed by external organisations;
- products or services offered by third parties;
- advertising appearing on external websites;
- software available from third-party websites;
- modifications made by third-party organisations after publication.

Visitors should independently evaluate information obtained from external sources before relying upon it.

18.13 Links to the Foundation's Website

Third parties may link to the Foundation's website provided that such linking:

- is lawful;
- is accurate;
- does not misrepresent the Foundation;
- does not imply endorsement where none exists;
- does not damage the Foundation's reputation;
- does not facilitate unlawful activity.

The Foundation reserves the right to request the removal of links that are misleading, inappropriate, or harmful to its reputation or mission.

18.14 International Third-Party Services

Some third-party service providers engaged by the Foundation may operate in jurisdictions outside the country where users reside.

Where personal information is transferred internationally through such services, the Foundation shall take reasonable steps to ensure that appropriate safeguards are implemented, consistent with **Section 13 – International Data Transfers** of this Privacy Policy.

18.15 Third-Party Compliance

The Foundation seeks to engage reputable organisations that demonstrate responsible information management practices.

Where appropriate, the Foundation may consider factors such as:

- information security standards;
- contractual confidentiality;
- operational reliability;
- regulatory compliance;
- organisational reputation;
- experience;
- safeguarding commitments;
- financial accountability.

However, the Foundation cannot guarantee the future conduct or compliance of independent third-party organisations.

18.16 Reporting Concerns Regarding Third-Party Services

Users who become aware of concerns relating to third-party services accessed through the Foundation's website are encouraged to notify the Foundation.

Examples include:

- broken or misleading links;
- suspected fraud;
- inappropriate content;
- security concerns;
- accessibility barriers;
- privacy concerns;
- suspected misuse of the Foundation's name or branding.

The Foundation shall review such reports and take appropriate action where reasonably practicable.

18.17 No Endorsement

Unless expressly stated otherwise, references to external organisations, websites, products, services, or technologies are provided solely for operational, informational, educational, fundraising, or partnership purposes.

Such references shall not be interpreted as an endorsement, recommendation, certification, or approval of any external organisation or its products or services.

18.18 Limitation of Responsibility

To the fullest extent permitted by applicable law, the Foundation shall not be responsible for:

- privacy practices of third-party organisations;
- security incidents occurring within third-party systems;
- content published by external websites;
- interruptions to third-party services;
- decisions made by independent organisations;
- losses arising from reliance upon third-party information or services, except where such liability cannot lawfully be excluded.

Nothing in this section limits any rights or remedies that may be available to individuals under applicable law.

18.19 Commitment to Responsible Digital Partnerships

Pneuma African Foundation values collaboration with trusted digital service providers, humanitarian partners, educational institutions, financial service providers, and technology organisations that support its mission.

The Foundation is committed to exercising reasonable care when selecting third-party providers, promoting responsible data governance, and encouraging transparency in all digital partnerships. By maintaining appropriate oversight, contractual safeguards, and periodic reviews of external relationships, the Foundation seeks to minimise privacy and security risks while ensuring that its website and online services remain effective, secure, and accessible to all users.

19. CHILDREN'S PRIVACY AND SAFEGUARDING

19.1 Introduction

Pneuma African Foundation is firmly committed to protecting the privacy, dignity, rights, and wellbeing of every child who comes into contact with the Foundation through its programmes, services, partnerships, digital platforms, fundraising activities, educational initiatives, humanitarian interventions, and community engagements.

The Foundation recognises that children are entitled to enhanced protection because they may be less aware of the risks associated with the collection and processing of personal information and may be particularly vulnerable to abuse, exploitation, neglect, trafficking, discrimination, or other forms of harm.

Accordingly, the Foundation adopts a child-centred approach to the collection, use, sharing, storage, and protection of children's personal information, ensuring that all processing activities are conducted in accordance with applicable laws, recognised safeguarding principles, and the Foundation's Child Safeguarding Policy and related governance documents.

19.2 Scope

This Section applies whenever the Foundation processes personal information relating to:

- children participating in Foundation programmes;

- children receiving humanitarian assistance;
- children attending Foundation events;
- children involved in educational or training activities;
- children featured in authorised publications or media;
- children participating in research or assessments;
- children supported through sponsorship or donor-funded initiatives;
- children interacting with the Foundation through its website or digital services.

It also applies to all Directors, employees, volunteers, consultants, contractors, interns, researchers, programme partners, and any other persons acting on behalf of the Foundation.

19.3 Best Interests of the Child

In all activities involving children, the Foundation shall treat the best interests of the child as a primary consideration.

When making decisions involving children's personal information, the Foundation shall consider:

- the child's safety and wellbeing;
- the child's dignity;
- the child's privacy;
- the child's age and level of maturity;
- the child's evolving capacities;
- the child's right to protection from harm;
- applicable legal requirements;
- safeguarding obligations.

Where there is any conflict between operational convenience and the protection of a child, safeguarding considerations shall take precedence.

19.4 Collection of Children's Personal Information

The Foundation shall collect children's personal information only where it is necessary for legitimate and lawful purposes, including:

- delivery of humanitarian assistance;
- education and child development programmes;
- health and nutrition initiatives;
- safeguarding and protection services;
- emergency response activities;
- programme registration;

- monitoring and evaluation;
- family tracing where appropriate;
- donor accountability;
- legal or regulatory compliance.

Only the minimum amount of personal information reasonably necessary shall be collected.

19.5 Lawful Basis for Processing Children's Information

Children's personal information shall be processed only where there is a lawful basis under applicable law.

Depending upon the circumstances, processing may be based upon:

- consent from a parent or legal guardian where required;
- the performance of humanitarian or charitable functions;
- compliance with legal obligations;
- protection of the vital interests of the child or another individual;
- safeguarding responsibilities;
- public interest activities;
- other lawful grounds recognised by applicable legislation.

The Foundation shall ensure that any reliance on consent or another lawful basis is appropriately documented where required.

19.6 Consent of Parents or Legal Guardians

Where applicable law requires parental or guardian consent, the Foundation shall obtain appropriate authorisation before collecting or processing a child's personal information.

Consent may be required for activities such as:

- programme participation;
- publication of identifiable photographs or videos;
- research projects;
- online services directed specifically at children;
- non-essential communications;
- other activities where required by law.

The Foundation may take reasonable steps to verify that consent has been provided by a parent or person legally authorised to act on behalf of the child.

19.7 Children's Participation

Where appropriate and having regard to the child's age, maturity, and understanding, the Foundation shall seek to explain:

- why information is being collected;
- how it will be used;
- who may receive it;
- how it will be protected;
- the child's rights regarding their information.

Information provided to children should be communicated in language that is clear, age-appropriate, and easy to understand.

19.8 Sensitive Information Relating to Children

The Foundation recognises that information concerning children is often highly sensitive.

Sensitive information may include:

- health information;
- disability information;
- educational records;
- safeguarding reports;
- protection assessments;
- psychosocial support records;
- family circumstances;
- emergency response records.

Such information shall receive enhanced protection and shall be accessible only to authorised individuals who require access for legitimate Foundation purposes.

19.9 Child Safeguarding and Confidentiality

All information relating to safeguarding concerns shall be handled with the highest degree of confidentiality consistent with the need to protect children.

The Foundation shall:

- restrict access to safeguarding records;
- maintain secure storage of safeguarding documentation;
- disclose information only to authorised persons;
- comply with mandatory reporting obligations where applicable;
- protect children from unnecessary exposure of personal information.

Confidentiality shall never prevent appropriate reporting or intervention where a child may be at risk of abuse, neglect, exploitation, or other harm.

19.10 Photographs, Videos, and Media Involving Children

The Foundation recognises that photographs, videos, audio recordings, and other media involving children require particular care.

Where children are featured in Foundation publications or communications, the Foundation shall:

- respect the dignity of every child;
- avoid exploitative or degrading portrayals;
- use images only for legitimate organisational purposes;
- obtain appropriate consent where required;
- avoid disclosing unnecessary identifying information;
- ensure that media does not place children at risk.

Images or stories shall never be used in a manner that compromises the safety, privacy, or dignity of a child.

19.11 Online Services Used by Children

Where children access Foundation-operated digital services, the Foundation shall take reasonable measures to:

- minimise the collection of personal information;
- maintain appropriate security controls;
- prevent unauthorised disclosure;
- provide age-appropriate information where practical;
- protect against cyber threats;
- monitor systems for security purposes.

The Foundation does not knowingly use children's personal information for commercial profiling or behavioural advertising.

19.12 Sharing Children's Personal Information

The Foundation shall share children's personal information only where necessary and lawful.

Information may be shared with:

- authorised safeguarding personnel;
- healthcare providers where appropriate;
- educational institutions where appropriate;
- humanitarian partners;
- government authorities where required by law;
- law enforcement agencies where necessary;
- courts or regulatory authorities where legally required.

Only the minimum amount of information necessary shall be disclosed.

19.13 Reporting Child Protection Concerns

Any Director, employee, volunteer, consultant, contractor, or partner who becomes aware of information suggesting that a child may be at risk of abuse, neglect, exploitation, trafficking, violence, or other harm shall report such concerns promptly through the Foundation's safeguarding procedures.

Reports shall be handled confidentially, professionally, and in accordance with applicable law and the Foundation's safeguarding policies.

19.14 Retention of Children's Information

Personal information relating to children shall be retained only for as long as necessary to fulfil the purposes for which it was collected or to comply with applicable legal, safeguarding, or regulatory requirements.

Where safeguarding responsibilities require extended retention, such records shall continue to receive enhanced protection and restricted access.

The retention and secure disposal of children's records shall be managed in accordance with **Section 15 – Data Retention and Secure Disposal** of this Privacy Policy.

19.15 Rights of Children and Parents or Legal Guardians

Subject to applicable law, children, parents, or legal guardians may exercise relevant privacy rights, including:

- requesting access to personal information;
- requesting correction of inaccurate information;
- requesting deletion where legally permissible;
- withdrawing consent where applicable;
- requesting restriction of processing;
- raising concerns regarding the handling of children's information.

The Foundation shall balance these rights with its safeguarding duties, legal obligations, and the best interests of the child.

19.16 Training and Awareness

The Foundation shall ensure that individuals working with or on behalf of the organisation receive appropriate safeguarding and privacy awareness training relevant to their responsibilities.

Training may include:

- child safeguarding principles;
- confidentiality obligations;
- recognising indicators of abuse or neglect;
- secure handling of children's personal information;
- reporting procedures;
- ethical communication involving children;
- applicable legal requirements.

The Foundation shall periodically review and update training materials to reflect evolving legal requirements, safeguarding standards, and organisational best practices.

19.17 Monitoring and Compliance

The Foundation shall monitor compliance with this Section through appropriate governance and oversight mechanisms.

Compliance activities may include:

- policy reviews;
- safeguarding audits;
- privacy compliance assessments;
- incident reviews;
- corrective actions;
- continuous improvement initiatives.

Any suspected misuse or unauthorised disclosure of children's personal information shall be investigated promptly, and appropriate remedial measures shall be taken.

19.18 Commitment to Protecting Children

Pneuma African Foundation believes that every child has the right to safety, dignity, privacy, and protection.

The Foundation is committed to embedding child safeguarding and privacy protection throughout its governance, programmes, partnerships, and digital operations. By implementing strong safeguarding measures, limiting the collection and use of children's personal information, and maintaining robust security and accountability practices, the Foundation seeks to create environments in which children are protected, respected, and empowered to thrive.

20. DATA BREACH NOTIFICATION AND INCIDENT RESPONSE

20.1 Introduction

Pneuma African Foundation recognises that despite implementing appropriate administrative, technical, physical, and organisational safeguards, security incidents and personal data breaches may occur.

The Foundation is committed to maintaining an effective incident response framework that enables the prompt identification, reporting, assessment, containment, investigation, mitigation, recovery, and documentation of actual or suspected personal data breaches.

The objectives of this framework are to:

- protect affected individuals from harm;
- minimise operational disruption;

- preserve the confidentiality, integrity, and availability of information;
- comply with applicable legal and regulatory obligations;
- maintain donor, beneficiary, volunteer, employee, partner, and public confidence; and
- continuously strengthen the Foundation's information security and privacy practices.

All persons acting on behalf of the Foundation share responsibility for reporting suspected incidents promptly and cooperating fully in incident response activities.

20.2 Purpose

The purpose of this Section is to establish a consistent and coordinated approach for:

- identifying personal data breaches;
 - reporting security incidents;
 - assessing the nature and severity of incidents;
 - containing and mitigating risks;
 - protecting affected individuals;
 - restoring normal operations;
 - notifying affected persons and competent authorities where required;
 - documenting incidents;
 - implementing corrective and preventive actions.
-

20.3 Scope

This Section applies to all actual or suspected incidents involving personal information processed by or on behalf of the Foundation, including information relating to:

- beneficiaries;
- donors;
- volunteers;
- employees;
- consultants;
- contractors;
- Board members;
- programme participants;
- suppliers;
- partner organisations;
- website users;
- research participants.

It applies regardless of whether information is stored:

- electronically;
- in paper records;

- in cloud environments;
 - on portable devices;
 - within third-party systems processing information on behalf of the Foundation.
-

20.4 Definition of a Personal Data Breach

For the purposes of this Privacy Policy, a personal data breach is any security incident that results in the accidental or unlawful:

- destruction;
- loss;
- alteration;
- unauthorised disclosure;
- unauthorised access;
- misuse;
- unavailability

of personal information processed by the Foundation.

A breach may arise from malicious acts, human error, technical failures, or natural disasters.

20.5 Examples of Personal Data Breaches

Examples of incidents that may constitute a personal data breach include:

- loss or theft of laptops, mobile phones, or storage devices containing personal information;
 - unauthorised access to Foundation systems;
 - phishing attacks resulting in compromised accounts;
 - ransomware or malware infections;
 - accidental disclosure of confidential information to the wrong recipient;
 - unauthorised publication of personal information;
 - destruction of records through fire, flooding, or other disasters;
 - insecure disposal of confidential records;
 - compromised passwords or authentication credentials;
 - unauthorised access by employees, volunteers, or contractors;
 - cyberattacks targeting the Foundation's website or digital platforms;
 - failures of third-party service providers resulting in unauthorised disclosure.
-

20.6 Immediate Reporting of Incidents

Every Director, employee, volunteer, consultant, contractor, intern, researcher, or authorised representative who becomes aware of an actual or suspected personal data breach shall report the matter immediately through the Foundation's established reporting procedures.

Reports should be made without unnecessary delay, regardless of whether:

- the breach appears minor;
- the full facts are known;
- harm has already occurred; or
- responsibility has been established.

Prompt reporting enables timely assessment and reduces the potential impact of the incident.

20.7 Initial Incident Assessment

Upon receiving a report of an actual or suspected breach, the Foundation shall conduct an initial assessment to determine:

- the nature of the incident;
- whether personal information has been affected;
- the categories of information involved;
- the number of individuals potentially affected;
- whether sensitive personal information is involved;
- whether children or vulnerable persons are affected;
- the likelihood of harm;
- immediate containment measures required;
- whether notification obligations may arise.

The Foundation shall document the findings of the initial assessment.

20.8 Incident Containment

The Foundation shall take appropriate steps to contain the incident and prevent further unauthorised access, disclosure, alteration, or loss of information.

Containment measures may include:

- disabling compromised accounts;
- changing passwords;
- isolating affected systems;
- disconnecting devices from networks;
- suspending affected services;
- recovering information from backups;
- revoking access permissions;

- blocking malicious network activity;
- preserving evidence for investigation.

Containment measures shall be proportionate to the nature and severity of the incident.

20.9 Investigation

Following containment, the Foundation shall conduct an appropriate investigation to determine:

- how the incident occurred;
- when the incident occurred;
- what information was affected;
- who was affected;
- whether the information was accessed or disclosed;
- the root cause of the incident;
- whether legal obligations have been triggered;
- whether additional security weaknesses exist.

Investigations shall be conducted fairly, objectively, and confidentially.

20.10 Risk Assessment

The Foundation shall assess the potential impact of each breach by considering factors such as:

- the sensitivity of the information involved;
- the volume of information affected;
- whether the information was encrypted or otherwise protected;
- the likelihood of misuse;
- the identity of any unauthorised recipients;
- potential financial harm;
- potential identity theft;
- reputational harm;
- risks to personal safety;
- safeguarding implications;
- operational disruption.

The outcome of the assessment shall guide decisions regarding notification and remedial action.

20.11 Notification of Affected Individuals

Where required by applicable law or where a breach is likely to result in a significant risk to the rights, freedoms, safety, or privacy of affected individuals, the Foundation shall notify those individuals without undue delay.

Such notification shall, where appropriate, include:

- a description of the incident;
- the categories of information affected;
- the likely consequences of the breach;
- measures already taken by the Foundation;
- recommended actions individuals may take to protect themselves;
- contact details for further information or assistance.

Notifications shall be communicated clearly, accurately, and in language that is reasonably understandable to the intended recipients.

20.12 Notification of Regulatory Authorities

Where applicable law requires notification of a competent supervisory, regulatory, or governmental authority, the Foundation shall provide such notification within the timeframe prescribed by the relevant legal requirements.

The Foundation shall cooperate fully with competent authorities during any investigation or regulatory review arising from a personal data breach.

20.13 Incidents Involving Children or Vulnerable Persons

Where a breach involves children's personal information or information relating to vulnerable individuals, the Foundation shall apply enhanced response measures.

Such measures may include:

- expedited investigation;
- immediate safeguarding assessment;
- notification of appropriate safeguarding personnel;
- engagement with parents or legal guardians where appropriate;
- reporting to relevant authorities where required by law;
- additional protective measures to reduce the risk of harm.

The protection and safety of affected children and vulnerable individuals shall remain a primary consideration throughout the incident response process.

20.14 Incidents Involving Third-Party Service Providers

Where a breach occurs within the systems of a third-party service provider processing information on behalf of the Foundation, the Foundation shall:

- require prompt notification from the service provider;
- assess the nature and impact of the breach;
- coordinate response activities where appropriate;
- review contractual obligations;
- determine whether notification obligations apply;
- evaluate the provider's response;
- consider whether continued engagement with the provider remains appropriate.

Third-party service providers shall be expected to cooperate fully in incident investigations affecting Foundation information.

20.15 Documentation and Record-Keeping

The Foundation shall maintain records of personal data breaches and significant security incidents, regardless of whether notification is required.

Incident records may include:

- the date of the incident;
- a description of the incident;
- affected systems;
- categories of information involved;
- number of affected individuals where known;
- investigation findings;
- actions taken;
- notifications issued;
- corrective measures implemented;
- lessons learned.

These records support accountability, governance, and continuous improvement.

20.16 Recovery and Restoration

Following containment and investigation, the Foundation shall take reasonable steps to restore affected systems and services.

Recovery activities may include:

- restoring data from secure backups;
- rebuilding compromised systems;
- implementing additional security controls;
- validating system integrity;
- testing restored services;
- strengthening monitoring measures;
- supporting affected individuals where appropriate.

Operational recovery shall prioritise the continuity of humanitarian programmes and essential organisational functions.

20.17 Corrective and Preventive Actions

Following each significant incident, the Foundation shall identify and implement corrective actions designed to reduce the likelihood of recurrence.

Corrective actions may include:

- updating security policies;
- improving technical safeguards;
- strengthening access controls;
- revising operational procedures;
- enhancing staff training;
- improving vendor oversight;
- updating risk assessments;
- implementing additional monitoring technologies.

Lessons learned from incidents shall be incorporated into the Foundation's ongoing risk management and governance processes.

20.18 Confidentiality During Incident Response

Information relating to security incidents and personal data breaches shall be treated as confidential.

Access to incident information shall be limited to individuals who require access for legitimate purposes, including:

- incident management;
- safeguarding;
- legal compliance;
- regulatory reporting;
- system recovery;
- governance oversight.

Confidentiality shall be maintained throughout the investigation, except where disclosure is required by law or necessary to protect affected individuals.

20.19 Training and Preparedness

The Foundation shall promote organisational preparedness through:

- incident response training;
- cybersecurity awareness programmes;
- periodic policy reviews;
- incident reporting guidance;
- tabletop exercises where appropriate;
- continuous improvement initiatives.

Employees, volunteers, consultants, and contractors shall understand their responsibilities for identifying and reporting suspected incidents promptly.

20.20 Governance and Oversight

The Board of Directors shall provide oversight of the Foundation's incident response framework.

Executive Management shall ensure that appropriate procedures, resources, and personnel are available to implement this Section.

All Directors, employees, volunteers, consultants, contractors, and authorised representatives shall comply with applicable incident reporting and response requirements.

Failure to report a known personal data breach or deliberate concealment of a security incident may result in disciplinary action, termination of contractual relationships, referral to competent authorities where appropriate, or other lawful measures.

20.21 Continuous Improvement

The Foundation shall periodically review and update its incident response procedures to reflect:

- evolving cybersecurity threats;
- technological developments;
- organisational changes;
- lessons learned from incidents;
- legal and regulatory developments;
- recognised industry best practices.

Regular reviews help ensure that the Foundation remains prepared to respond effectively to emerging privacy and information security risks.

20.22 Commitment to Responsible Incident Management

Pneuma African Foundation is committed to responding to personal data breaches with transparency, professionalism, and accountability.

Through timely reporting, effective containment, thorough investigation, appropriate notification, and continuous improvement, the Foundation seeks to minimise harm, maintain public confidence, and fulfil its responsibility to protect the personal information entrusted to its care.

Recognising that information security is an ongoing process rather than a single event, the Foundation will continue to strengthen its incident response capabilities and foster a culture of vigilance, resilience, and responsible stewardship across all areas of its operations.

21. CHANGES TO THIS PRIVACY POLICY

21.1 Introduction

Pneuma African Foundation is committed to ensuring that this Privacy Policy remains accurate, relevant, effective, and consistent with evolving legal requirements, organisational practices, technological developments, and recognised standards for privacy and data protection.

As the Foundation expands its programmes, introduces new services, adopts new technologies, or responds to changes in applicable legislation, it may become necessary to amend this Privacy Policy.

This Section explains how the Foundation reviews, updates, approves, publishes, and communicates changes to this Privacy Policy.

21.2 Commitment to Continuous Review

The Foundation shall periodically review this Privacy Policy to ensure that it continues to:

- reflect current organisational practices;
- comply with applicable laws and regulations;
- address emerging privacy risks;
- support technological developments;
- align with organisational governance standards;
- protect the rights of individuals;
- maintain transparency and accountability.

Policy reviews shall form part of the Foundation's broader governance, compliance, and risk management framework.

21.3 Circumstances Requiring Policy Updates

The Foundation may revise this Privacy Policy for reasons including, but not limited to:

- changes in applicable data protection legislation;
- new regulatory guidance;
- organisational restructuring;
- expansion of Foundation programmes or services;
- introduction of new digital platforms;
- implementation of new technologies;
- changes in information security practices;
- adoption of new fundraising methods;
- changes in payment processing systems;
- modifications to online services;
- recommendations arising from audits or compliance reviews;
- lessons learned from privacy or security incidents;
- updates to safeguarding practices;
- changes in donor or contractual requirements.

Not every operational change will require an amendment to this Privacy Policy. The Foundation shall determine whether revisions are necessary based on the significance of the change.

21.4 Periodic Policy Review

As part of good governance, the Foundation shall conduct formal reviews of this Privacy Policy at regular intervals.

Unless an earlier review is required, this Privacy Policy shall ordinarily be reviewed:

- at least once every two (2) years;
- following significant legislative or regulatory changes;
- after major organisational changes;
- following significant privacy or cybersecurity incidents;
- when introducing new categories of personal information processing;
- whenever otherwise considered necessary by the Foundation.

Additional interim reviews may be undertaken where appropriate.

21.5 Approval of Policy Changes

All significant amendments to this Privacy Policy shall be subject to appropriate internal review and approval before implementation.

Depending on the nature of the amendment, approval may be provided by:

- the Board of Directors;
- the Executive Director;
- Executive Management;
- authorised governance committees;
- designated officers responsible for privacy, compliance, or information governance.

No amendment shall take effect until it has been duly approved in accordance with the Foundation's governance procedures.

21.6 Version Control

To promote transparency and accountability, the Foundation shall maintain appropriate version control for this Privacy Policy.

Version control information may include:

- document title;
- version number;
- approval date;
- effective date;
- review date;
- approving authority;
- summary of significant amendments.

Superseded versions may be retained in accordance with the Foundation's records management and document retention procedures.

21.7 Effective Date

Each version of this Privacy Policy shall specify the date on which it becomes effective.

Unless otherwise stated, revisions shall take effect from the effective date indicated within the Policy.

The effective date shall be clearly displayed on the document to enable users to identify the version currently in force.

21.8 Notification of Changes

Where appropriate, the Foundation shall take reasonable steps to inform users of significant changes to this Privacy Policy.

Notification methods may include:

- publication on the Foundation's website;
- updates within online services;
- email notifications where appropriate;
- donor communications;
- volunteer communications;
- employee communications;
- notices provided during programme registration;
- other appropriate communication channels.

The method of notification shall be proportionate to the significance of the changes.

21.9 Material Changes

Where amendments materially affect the way personal information is collected, used, shared, or protected, the Foundation shall take reasonable steps to provide clear notice before or at the time such changes become effective, where required by applicable law.

Examples of material changes may include:

- introduction of new categories of personal information;
- new purposes for processing;
- significant changes to international data transfers;
- changes affecting individuals' privacy rights;
- introduction of new technologies involving personal information;
- significant revisions to information-sharing practices.

Where required by law, the Foundation shall obtain any necessary consent before implementing material changes.

21.10 Minor Administrative Changes

Not every revision constitutes a material change.

Administrative updates may include:

- correction of typographical errors;
- clarification of wording;
- updated contact details;
- formatting improvements;
- internal cross-reference updates;
- organisational branding updates;
- revisions that do not materially affect individuals' rights or the Foundation's processing activities.

Such administrative changes may be implemented without separate notice, although the updated version shall continue to be published on the Foundation's website.

21.11 User Responsibility

Individuals are encouraged to review this Privacy Policy periodically to remain informed about how the Foundation protects personal information.

Continued use of the Foundation's website, services, programmes, or digital platforms after the effective date of an updated Privacy Policy constitutes acknowledgement that the revised Policy applies to future interactions, to the extent permitted by applicable law.

Where applicable law requires express consent for certain changes, the Foundation shall obtain such consent before relying upon the updated provisions.

21.12 Historical Versions

The Foundation may retain previous versions of this Privacy Policy for:

- governance purposes;
- legal compliance;
- audit requirements;
- organisational records;
- historical reference;
- dispute resolution.

Where appropriate, historical versions may be made available upon reasonable request, subject to operational considerations and applicable legal requirements.

21.13 Interaction with Other Policies

This Privacy Policy forms part of the Foundation's broader governance framework and should be read together with other applicable organisational policies, including but not limited to:

- Terms and Conditions;
- Cookie Policy;
- Data Protection Policy;
- Information Security Policy;
- Child Safeguarding Policy;
- Code of Conduct;
- Records Management Policy;
- Acceptable Use Policy;
- Incident Response Policy;
- Whistleblower Policy.

Where another organisational policy establishes more specific requirements relating to a particular activity, that policy shall apply in conjunction with this Privacy Policy.

21.14 Continued Compliance

The Foundation shall make reasonable efforts to ensure that any amendments to this Privacy Policy continue to reflect:

- applicable legal obligations;
- recognised privacy principles;
- organisational values;
- humanitarian best practices;
- safeguarding commitments;
- information security standards;
- principles of transparency and accountability.

The Foundation shall not amend this Privacy Policy in a manner that diminishes legal rights afforded to individuals under applicable law.

21.15 Accessibility of Updated Policies

The current version of this Privacy Policy shall be made available through appropriate channels, including the Foundation's official website.

Where reasonably practicable, the Policy shall be presented in a format that is:

- clear and understandable;
- accessible to a broad audience;
- compatible with commonly used digital devices;
- readily available without unreasonable barriers to access.

The Foundation shall endeavour to ensure that individuals can easily identify the most current version of the Policy.

21.16 Commitment to Transparency

Pneuma African Foundation believes that transparency is essential to maintaining the confidence of donors, beneficiaries, volunteers, employees, partners, regulators, and the communities it serves.

The Foundation is committed to communicating changes to this Privacy Policy openly, maintaining accurate version control, and ensuring that individuals remain informed about how their personal information is collected, used, shared, protected, and managed.

By regularly reviewing and updating this Privacy Policy, the Foundation seeks to uphold the highest standards of privacy governance, accountability, and responsible stewardship of personal information.

22. GOVERNING LAW AND JURISDICTION

22.1 Introduction

This Privacy Policy shall be interpreted and applied in accordance with the applicable laws governing the operations of Pneuma African Foundation and the processing of personal information within the jurisdictions in which the Foundation conducts its activities.

The Foundation is committed to complying with all applicable privacy, data protection, cybersecurity, safeguarding, charitable, employment, financial, and other legal requirements relevant to its operations. Where the Foundation conducts activities across multiple jurisdictions, it shall take reasonable steps to comply with the legal obligations applicable to those activities.

This Section establishes the legal framework governing the interpretation, implementation, and enforcement of this Privacy Policy.

22.2 Applicable Law

This Privacy Policy shall be governed by:

- the laws of the Republic of Uganda, where the Foundation is established and principally operates;
- applicable data protection and privacy legislation;
- laws regulating charitable and non-profit organisations;
- employment legislation where applicable;
- financial reporting and anti-money laundering requirements where applicable;
- child protection and safeguarding legislation;
- cybersecurity and electronic communications laws;
- any other applicable statutory or regulatory requirements relevant to the Foundation's activities.

Where the Foundation operates internationally or collaborates with international partners, additional legal obligations may apply to specific programmes, projects, or processing activities.

22.3 Compliance with Data Protection Laws

The Foundation shall process personal information in accordance with applicable data protection and privacy laws governing the jurisdictions in which it operates.

Where different legal requirements apply to particular processing activities, the Foundation shall seek to implement procedures that satisfy the applicable legal standards while maintaining consistent principles of:

- lawfulness;
- fairness;
- transparency;
- accountability;
- purpose limitation;
- data minimisation;
- accuracy;
- integrity and confidentiality;
- responsible governance.

Where two or more legal requirements apply simultaneously, the Foundation shall seek to comply with the higher standard to the extent permitted by law.

22.4 International Operations

As an organisation engaged in humanitarian, development, educational, and charitable activities, the Foundation may conduct programmes or collaborate with partners in multiple countries.

Accordingly:

- different legal systems may apply to specific projects;
- contractual obligations may impose additional privacy requirements;
- donor agreements may establish supplementary compliance obligations;
- international data transfers shall be governed in accordance with **Section 13 – International Data Transfers** of this Privacy Policy.

The Foundation shall take reasonable steps to ensure that cross-border activities are conducted consistently with applicable legal obligations.

22.5 Interpretation of this Privacy Policy

This Privacy Policy shall be interpreted:

- in good faith;
- consistently with applicable law;
- in a manner that promotes the protection of personal information;
- in support of the Foundation's humanitarian and charitable mission;
- with due regard to recognised privacy and information governance principles.

Headings and section titles are included for convenience only and shall not affect the interpretation of this Privacy Policy.

Where uncertainty exists regarding the interpretation of any provision, the interpretation that best protects the lawful rights and privacy of individuals, while remaining consistent with applicable law and the Foundation's legitimate operational responsibilities, shall generally be preferred.

22.6 Relationship with Applicable Law

Nothing contained in this Privacy Policy shall be interpreted as limiting or excluding any rights, protections, or obligations established by applicable law.

Where any provision of this Privacy Policy conflicts with mandatory legal requirements, the applicable law shall prevail to the extent of the inconsistency.

The remaining provisions of this Privacy Policy shall continue to apply unless rendered invalid or unenforceable by operation of law.

22.7 Compliance with Regulatory Authorities

The Foundation shall cooperate with competent governmental, regulatory, supervisory, judicial, or law enforcement authorities where required by applicable law.

Such cooperation may include:

- responding to lawful information requests;
- participating in investigations;
- complying with court orders;
- fulfilling statutory reporting obligations;
- implementing regulatory directives;
- supporting safeguarding investigations;
- responding to legally authorised audits.

The Foundation shall disclose personal information only where disclosure is lawful, necessary, and proportionate.

22.8 Dispute Resolution

The Foundation encourages individuals to raise privacy concerns directly with the Foundation before initiating formal legal proceedings.

Where a concern arises regarding the handling of personal information, the Foundation shall seek to resolve the matter through:

- open communication;
- prompt investigation;
- fair consideration of the facts;
- appropriate remedial action where necessary;
- internal complaint procedures.

The Foundation believes that many privacy concerns can be resolved efficiently through constructive dialogue and cooperation.

22.9 Regulatory Complaints

Nothing in this Privacy Policy prevents an individual from exercising any legal right to submit a complaint to a competent data protection authority, privacy regulator, or other supervisory authority where such rights exist under applicable law.

The Foundation shall cooperate with competent authorities during any lawful investigation relating to privacy or data protection matters.

22.10 Jurisdiction of Competent Courts

Subject to any mandatory legal requirements or contractual arrangements providing otherwise, disputes arising from or relating to this Privacy Policy shall be subject to the jurisdiction of the competent courts of the Republic of Uganda.

Where legal proceedings arise in connection with the Foundation's international activities, the applicable jurisdiction may be determined by:

- relevant legislation;
- contractual agreements;
- applicable international legal principles;
- mandatory requirements of the relevant jurisdiction.

Nothing in this Privacy Policy limits any rights that individuals may have under mandatory provisions of applicable law.

22.11 Cross-Border Legal Obligations

Where the Foundation processes personal information across national borders, it shall seek to comply with applicable legal obligations relating to:

- international data transfers;
- contractual confidentiality;
- safeguarding;
- donor accountability;
- financial reporting;
- anti-fraud measures;
- cybersecurity;
- records management.

The Foundation shall implement appropriate governance measures to support compliance across multiple jurisdictions.

22.12 Severability

If any provision of this Privacy Policy is determined by a court or competent authority to be unlawful, invalid, or unenforceable, that provision shall, to the extent necessary, be severed from the remaining provisions.

The remaining provisions shall continue in full force and effect, provided that the overall purpose and operation of this Privacy Policy are not materially affected.

22.13 Waiver

Failure by the Foundation to enforce any provision of this Privacy Policy shall not constitute a waiver of that provision or of any other rights available to the Foundation under applicable law.

Any waiver shall be effective only if made expressly and in writing by an authorised representative of the Foundation.

22.14 Language

This Privacy Policy is prepared in the English language.

Where translations are provided for convenience, the English version shall prevail in the event of any inconsistency or ambiguity, unless otherwise required by applicable law.

The Foundation may make translated versions available to improve accessibility for programme participants and communities where appropriate.

22.15 Relationship with Contracts and Other Policies

This Privacy Policy operates alongside the Foundation's other governance documents, policies, procedures, contractual agreements, and applicable legal obligations.

Where an individual enters into a separate written agreement with the Foundation containing privacy-related provisions, those contractual provisions shall apply in addition to this Privacy Policy.

Where inconsistencies arise, the Foundation shall seek to interpret the relevant documents harmoniously and in accordance with applicable law.

22.16 No Limitation of Statutory Rights

Nothing in this Privacy Policy shall exclude, restrict, or limit any statutory rights available to individuals under applicable data protection, consumer protection, employment, safeguarding, or other relevant legislation.

Individuals shall continue to enjoy all rights and remedies provided by applicable law, irrespective of the provisions of this Privacy Policy.

22.17 Commitment to Legal Compliance and Good Governance

Pneuma African Foundation is committed to operating with integrity, transparency, accountability, and respect for the rule of law.

The Foundation recognises that effective privacy protection depends upon sound governance, compliance with applicable legal requirements, responsible stewardship of personal information, and ongoing engagement with recognised standards of information management.

By adopting this Privacy Policy, the Foundation affirms its commitment to conducting all activities in a lawful, ethical, and responsible manner while respecting the rights, dignity, and privacy of every individual whose personal information it processes.

23. CONTACT INFORMATION AND PRIVACY ENQUIRIES

23.1 Introduction

Pneuma African Foundation is committed to maintaining open, transparent, and accessible communication regarding the collection, use, protection, and management of personal information.

Individuals who have questions, concerns, requests, or complaints relating to this Privacy Policy or the Foundation's privacy practices are encouraged to contact the Foundation using the contact information provided in this Section.

The Foundation is committed to responding to privacy enquiries professionally, respectfully, and within a reasonable timeframe, while complying with applicable legal and regulatory obligations.

23.2 Contacting the Foundation

Individuals may contact the Foundation regarding any matter relating to privacy or data protection, including:

- requests to exercise privacy rights;
- requests for access to personal information;
- requests to correct inaccurate information;
- requests for deletion where applicable;
- requests to restrict processing;
- withdrawal of consent;
- objections to processing;
- privacy complaints;
- questions regarding this Privacy Policy;
- reports of suspected personal data breaches;
- safeguarding-related privacy concerns;
- concerns regarding website privacy practices.

The Foundation welcomes constructive enquiries and is committed to resolving concerns fairly and transparently.

23.3 Privacy Contact Details

Privacy-related enquiries should be directed to the Foundation through its official contact channels.

Pneuma African Foundation

Registered Office:
Kampala, Uganda

Email:
privacy@pneumaafricanfoundation.org

General Enquiries:
info@pneumaafricanfoundation.org

Website:
www.pneumaafricanfoundation.org

Where a dedicated Data Protection Officer or Privacy Officer has been appointed, the Foundation may publish the relevant contact details on its official website or through other appropriate communication channels.

23.4 Information to Include in Your Request

To assist the Foundation in responding efficiently, individuals are encouraged to include:

- full name;
- preferred contact details;
- sufficient information to identify the relevant records;
- a clear description of the request or concern;
- dates or reference numbers where applicable;
- supporting documentation where appropriate.

Providing complete information helps the Foundation process requests more accurately and efficiently.

23.5 Identity Verification

Before responding to certain requests involving personal information, the Foundation may require reasonable verification of the identity of the requesting individual.

Identity verification helps protect individuals against:

- identity theft;
- unauthorised disclosure;
- fraud;
- impersonation;
- misuse of personal information.

The Foundation may request additional documentation where necessary to verify identity before releasing confidential information or making changes to personal records.

Verification procedures shall be proportionate to the sensitivity of the information requested.

23.6 Response Time

The Foundation shall acknowledge receipt of privacy-related enquiries as soon as reasonably practicable.

The Foundation shall endeavour to respond within a reasonable period, taking into account:

- the complexity of the request;
- the volume of information involved;
- applicable legal requirements;
- operational circumstances;
- safeguarding considerations where relevant.

Where additional time is reasonably required, the Foundation shall, where appropriate, inform the individual of the reason for the delay and provide an estimated timeframe for a substantive response.

23.7 Privacy Complaints

Individuals who believe that the Foundation has not handled personal information appropriately are encouraged to submit a complaint.

Complaints should include, where possible:

- a description of the concern;

- relevant dates;
- supporting documentation;
- details of any previous correspondence;
- the outcome sought by the complainant.

The Foundation shall:

- acknowledge receipt of the complaint;
- review the matter impartially;
- investigate the circumstances where appropriate;
- communicate its findings;
- implement corrective measures where necessary;
- maintain appropriate records of complaints and their resolution.

The Foundation values complaints as an opportunity to improve its privacy practices and organisational governance.

23.8 Reports of Personal Data Breaches

Individuals who become aware of an actual or suspected personal data breach involving the Foundation are encouraged to notify the Foundation without unnecessary delay.

Reports may include concerns regarding:

- unauthorised disclosure of personal information;
- suspicious emails or communications;
- phishing attempts;
- lost or stolen Foundation devices;
- compromised user accounts;
- accidental disclosure;
- website security concerns;
- suspected cyberattacks;
- misuse of Foundation information.

Prompt reporting enables the Foundation to investigate, contain, and respond to incidents effectively in accordance with **Section 20 – Data Breach Notification and Incident Response**.

23.9 Safeguarding-Related Privacy Concerns

Where a privacy concern involves a child, vulnerable person, safeguarding matter, or suspected abuse, the Foundation shall treat the matter with the highest priority and confidentiality, consistent with its legal and safeguarding responsibilities.

Individuals should report safeguarding concerns immediately through the Foundation's designated safeguarding procedures.

The Foundation shall take appropriate action to protect children and vulnerable individuals while maintaining confidentiality to the fullest extent consistent with applicable law and safeguarding obligations.

23.10 Communications by Electronic Means

Privacy enquiries may be submitted electronically using the Foundation's published communication channels.

When communicating electronically, individuals are encouraged to:

- use official Foundation email addresses;
- avoid sending unnecessary sensitive personal information;
- verify the authenticity of communications purporting to originate from the Foundation;
- notify the Foundation if fraudulent communications are suspected.

The Foundation shall take reasonable steps to protect electronic communications but cannot guarantee the absolute security of information transmitted over the internet.

23.11 Communications by Post or In Person

Where appropriate, individuals may also submit written privacy requests by post or deliver them in person to the Foundation's registered office or another officially designated location.

Current postal addresses and office locations shall be published on the Foundation's official website and updated as necessary.

The Foundation encourages individuals to verify current contact details before sending correspondence.

23.12 Regulatory Authorities

If an individual remains dissatisfied after the Foundation has considered a privacy concern, they may have the right, subject to applicable law, to submit a complaint to the competent data protection or privacy supervisory authority in the relevant jurisdiction.

Nothing in this Privacy Policy limits any statutory rights that individuals may have to seek assistance from competent regulatory authorities or pursue remedies available under applicable law.

The Foundation shall cooperate with lawful enquiries and investigations conducted by competent authorities.

23.13 Accessibility and Communication Assistance

The Foundation is committed to making its privacy information reasonably accessible to all individuals.

Where reasonably practicable, the Foundation may provide assistance to individuals who require support in understanding this Privacy Policy or exercising their privacy rights due to:

- disability;
- language barriers;
- literacy challenges;
- age-related needs;
- other reasonable accessibility requirements.

Requests for communication assistance shall be considered fairly and in accordance with the Foundation's commitment to inclusion and equal opportunity.

23.14 Updates to Contact Information

The Foundation may update its contact details from time to time to reflect organisational changes.

Current contact information shall be maintained on the Foundation's official website.

Individuals are encouraged to refer to the most recent version of this Privacy Policy or the Foundation's website to ensure that enquiries are directed to the correct contact channels.

23.15 Good Faith Communications

The Foundation encourages all individuals to submit privacy enquiries, requests, and complaints in good faith.

Similarly, the Foundation shall:

- treat all communications respectfully;
- consider requests fairly;
- protect confidential information;
- avoid unnecessary delay;
- communicate clearly regarding the outcome of requests.

The Foundation reserves the right to decline requests that are manifestly unfounded, abusive, repetitive, or otherwise permitted to be refused under applicable law, while providing reasons where required.

23.16 Commitment to Open Communication

Pneuma African Foundation believes that effective privacy governance depends upon open communication, accountability, and mutual trust.

The Foundation is committed to maintaining accessible channels through which donors, beneficiaries, volunteers, employees, partners, website users, and members of the public may raise questions, exercise their privacy rights, report concerns, or seek clarification regarding the handling of personal information.

By responding promptly, respectfully, and transparently to privacy-related communications, the Foundation seeks to strengthen public confidence and uphold its commitment to responsible stewardship of personal information.

24. FINAL PROVISIONS

24.1 Introduction

This Privacy Policy constitutes the official statement of Pneuma African Foundation regarding the collection, use, disclosure, storage, protection, retention, and management of personal information processed through its programmes, services, website, digital platforms, partnerships, fundraising activities, and organisational operations.

This Policy reflects the Foundation's commitment to responsible governance, transparency, accountability, respect for human dignity, and the lawful protection of personal information entrusted to its care.

All persons acting on behalf of the Foundation are expected to comply with this Privacy Policy and to support its effective implementation throughout the organisation.

24.2 Status of this Privacy Policy

This Privacy Policy is an official governance document adopted by Pneuma African Foundation.

It establishes the Foundation's organisational standards for privacy and information governance and applies to all activities involving the processing of personal information unless superseded by applicable law or a more specific organisational policy addressing a particular processing activity.

This Policy should be read together with the Foundation's related governance documents, including:

- Terms and Conditions;
- Cookie Policy;
- Data Protection Policy;
- Information Security Policy;
- Child Safeguarding Policy;
- Code of Conduct;
- Records Management Policy;
- Acceptable Use Policy;
- Incident Response Policy;
- Whistleblower Policy; and
- other applicable organisational policies and procedures.

24.3 Implementation

The Foundation shall implement this Privacy Policy through appropriate:

- governance structures;
- operational procedures;
- organisational policies;
- staff guidance;
- volunteer orientation;
- contractual arrangements;
- security controls;
- records management practices;
- compliance monitoring;
- periodic training programmes.

Executive Management shall ensure that reasonable resources are available to support the effective implementation and maintenance of this Privacy Policy.

24.4 Responsibilities

The successful implementation of this Privacy Policy requires the cooperation of all persons acting on behalf of the Foundation.

Board of Directors

The Board of Directors shall:

- provide governance oversight;
- approve significant policy revisions where appropriate;
- promote organisational accountability;
- support compliance with applicable legal obligations.

Executive Management

Executive Management shall:

- oversee implementation of the Policy;
- allocate appropriate resources;
- ensure organisational compliance;
- promote a culture of privacy and information security.

Employees, Volunteers, Consultants, and Contractors

Every employee, volunteer, consultant, contractor, intern, researcher, and authorised representative shall:

- comply with this Privacy Policy;
- protect confidential information;
- report privacy concerns promptly;
- complete relevant training where required;
- cooperate with compliance activities;
- safeguard personal information at all times.

Failure to comply with this Privacy Policy may result in disciplinary action, termination of employment or contractual relationships, withdrawal of volunteer responsibilities, or other lawful measures, depending upon the circumstances.

24.5 Relationship with Other Organisational Documents

This Privacy Policy forms part of the Foundation's broader governance framework.

Where another approved organisational policy establishes more detailed requirements relating to a specific activity, that policy shall be read together with this Privacy Policy.

Examples include policies relating to:

- safeguarding;
- information security;
- records management;
- complaints handling;
- whistleblowing;
- fraud prevention;
- digital communications;
- procurement;
- volunteer management;
- human resources.

Where inconsistencies arise, the Foundation shall interpret these documents harmoniously and in accordance with applicable law.

24.6 No Waiver

Failure by the Foundation to enforce any provision of this Privacy Policy shall not constitute a waiver of any rights available to the Foundation under this Policy or applicable law.

Any waiver shall be valid only if expressly authorised in writing by an appropriately authorised representative of the Foundation.

A waiver relating to one matter shall not constitute a waiver relating to any other matter.

24.7 Severability

If any provision of this Privacy Policy is determined by a competent court, tribunal, or regulatory authority to be invalid, unlawful, or unenforceable, that provision shall, to the extent necessary, be severed from the remainder of the Policy.

The remaining provisions shall continue in full force and effect provided that the overall purpose and operation of the Privacy Policy are not materially affected.

24.8 Entire Privacy Policy

This Privacy Policy constitutes the Foundation's complete statement regarding its general privacy and personal information management practices.

It supersedes any previous versions of this Privacy Policy from the effective date specified in the document.

Nothing in this Section limits:

- statutory rights available to individuals;
- contractual obligations separately agreed with individuals;
- mandatory legal requirements;
- regulatory obligations applicable to the Foundation.

24.9 Good Faith Interpretation

This Privacy Policy shall be interpreted in good faith and in a manner consistent with:

- applicable law;
- recognised privacy principles;
- responsible governance;
- humanitarian values;
- safeguarding commitments;
- transparency;
- accountability;
- ethical stewardship.

Where ambiguity exists, the Foundation shall seek an interpretation that best protects the lawful rights and interests of individuals while enabling the Foundation to fulfil its legitimate charitable and humanitarian purposes.

24.10 Limitation of this Privacy Policy

This Privacy Policy explains how the Foundation generally manages personal information.

It does not:

- create contractual rights beyond those provided by applicable law;
- limit statutory rights available to individuals;
- replace applicable legislation;

- prevent the Foundation from complying with lawful requests made by competent authorities;
- prevent the Foundation from taking reasonable measures to protect individuals, communities, or organisational assets.

Where applicable law provides greater protections than this Privacy Policy, the applicable law shall prevail.

24.11 Organisational Commitment

Pneuma African Foundation recognises that responsible privacy management is fundamental to public trust, effective humanitarian action, and sound organisational governance.

The Foundation therefore commits to:

- respecting the dignity and privacy of every individual;
- collecting only information necessary for legitimate purposes;
- maintaining appropriate security safeguards;
- processing personal information lawfully and fairly;
- protecting confidential information;
- promoting transparency;
- responding appropriately to privacy concerns;
- continuously improving organisational privacy practices;
- fostering a culture of accountability and ethical responsibility.

These commitments guide the Foundation's interactions with beneficiaries, donors, volunteers, employees, partners, regulators, and members of the public.

24.12 Periodic Improvement

The Foundation recognises that privacy governance is an ongoing process requiring continuous review and improvement.

Accordingly, the Foundation shall periodically:

- review organisational privacy practices;
- assess emerging privacy risks;
- evaluate technological developments;
- strengthen security measures;
- update governance documents;
- improve staff awareness;
- enhance operational procedures;
- incorporate lessons learned from audits, incidents, and stakeholder feedback.

Continuous improvement supports the Foundation's long-term commitment to responsible stewardship of personal information.

24.13 Effective Date

This Privacy Policy shall take effect on the **Effective Date** specified on the document cover or in the document control section.

From that date, all Foundation personnel and authorised representatives shall conduct activities involving personal information in accordance with this Privacy Policy and any related organisational procedures.

Previous versions of this Privacy Policy shall be deemed superseded from the Effective Date unless otherwise expressly stated.

24.14 Acknowledgement of Organisational Commitment

By publishing this Privacy Policy, Pneuma African Foundation affirms its commitment to protecting the privacy, dignity, and rights of every individual whose personal information it processes.

The Foundation recognises that privacy protection is not merely a legal obligation but also a reflection of its core organisational values of integrity, accountability, compassion, respect, and responsible stewardship.

The Foundation remains committed to maintaining the confidence of donors, beneficiaries, volunteers, employees, partners, and the communities it serves by ensuring that personal information is managed with professionalism, transparency, fairness, and care.

24.15 Closing Statement

Pneuma African Foundation is dedicated to advancing sustainable development, humanitarian assistance, community empowerment, and social transformation across Africa.

The Foundation believes that responsible stewardship of personal information is essential to fulfilling this mission. By maintaining strong governance, implementing effective security measures, respecting individual privacy rights, and continuously strengthening its information management practices, the Foundation seeks to build lasting trust with every person and organisation it serves.

Privacy protection is an integral part of the Foundation's commitment to ethical leadership, responsible governance, and excellence in humanitarian service.

