Foreword

At Save The Pastoralists Kenya (STP), our mission is built on trust, trust with the communities we serve, our partners, our donors, and our colleagues. As stewards of sensitive information, it is our collective duty to uphold the highest standards of confidentiality, ensuring that personal, operational, and strategic data is protected at all times.

This Secrecy and Confidentiality Policy reflects our deep commitment to ethical conduct, transparency, and respect for privacy. It provides a f ramework for how we handle confidential information across all departments and levels of engagement, outlining our responsibilities and the safeguards we have in place.

In today's interconnected world, where information can be accessed, shared, and misused more easily than ever, safeguarding data is not just a legal obligation; it is a moral imperative. This policy will help us ensure that our operations remain secure, our relationships remain strong, and our impact remains focused on what matters most: the well-being and dignity of the pastoralists' communities we serve.

All staff, partners, and collaborators are encouraged to read this policy carefully, adhere to its guidelines, and seek clarification when needed. Upholding confidentiality is not the responsibility of a few, it is the responsibility of us all.

Christopher Eporon Ekuwom,

Executive Director, Save The Pastoralists Kenya (STP)

15Th April 2025.

Signature: _____

SAVE THE PASTORALISTS (STP) KENYA
19 APRIL 2025
P.O. BOX 438-30500 LODWAR

Policy Guiding Principles.

1. Understand and Classify Information

Not all information should be treated the same. It is important to separate public information from private and sensitive data. Key issues include failure to identify what is confidential, sharing sensitive details in public settings, or giving access to people who don't need it for their work.

2. Assign Responsibility Based on Role

Different people in the organization have different responsibilities. Some roles require access to sensitive information, while others do not. Problems arise when there is no clear policy about who can access what, when people aren't trained on confidentiality, or when everyone is given the same level of access without considering their duties.

3. Make Confidentiality a Core Value

Confidentiality should not only be a rule but a part of the organizat ion's identity and culture. It reflects integrity, trust, and our commitment to serve with respect and love. Issues can occur when staff and volunteers don't understand the importance of confidentiality, when it's seen only as a legal matter, or when it's not reinforced through faith -based values and everyday behavior.

1. Introduction.

Save The Pastoralists (STP) is a humanitarian and development -focused organization committed to safeguarding the dignity, privacy, and security of the communities and stakeho lders it serves. As part of our ethical and operational standards, we treat all confidential and sensitive information with the utmost care and discretion. This Secrecy and Confidentiality Policy outlines STP's principles, responsibilities, procedures, and measures to ensure the secure handling, use, and sharing of confidential information across all departments and at every level of the organization.

This policy serves as a critical framework for protecting personal, financial, operational, and legal information vital to STP's work, integrity, reputation, and effectiveness.

2. Defining Confidential Information.

Confidential information refers to any data, document, or communication —written, spoken, or electronic—that is not publicly available and, if disclosed without authorization, could harm the interests of STP, its partners, employees, beneficiaries, or donors. Such information includes, but is not limited to:

- Personal data of employees, volunteers, and beneficiaries, including names, addresses, I D numbers, medical information, or other identifiers.
- Financial records such as payroll data, donor information, budgets, audit reports, annual financial statements, bank statements, and bank details.
- Internal communications including emails, reports, stra tegy documents, and minutes of meetings.
- Legal and contractual documents, including Memoranda of Understanding (MOUs), contracts, partnership agreements, and pending negotiations.
- Proprietary methodologies, research findings, project evaluations, and any i ntellectual property created by or for STP.
- Information entrusted to STP by third parties under a confidentiality agreement or with an understanding of privacy.

3. Scope and Legal Obligations.

This policy applies to all individuals who are directly or in directly engaged with STP, including full-time and part-time employees, board members, interns, consultants, volunteers, and third-party service providers. It is enforceable from the beginning of a person's engagement with STP and remains binding even afte r the individual's association with the organization has ended.

STP operates under a range of legal and regulatory frameworks depending on the region. This policy is aligned with applicable data protection laws, labor regulations, and contractual confidentiality clauses. Violations may lead to disciplinary measures or legal proceedings depending on the nature and gravity of the offense.

4. Responsibilities and Obligations.

Every person associated with STP has a responsibility to protect confidential infor mation against unauthorized access, disclosure, or misuse. The following obligations are expected of all personnel:

- Access and use confidential information strictly for work -related purposes.
- Secure personal and organizational devices with strong passwords and lock screens when not in use.
- Refrain from discussing sensitive matters in public, on unsecured lines, or through personal devices.
- Report any suspected or actual breach of confidentiality to the appropriate authority immediately.
- Handle printed or written materials containing sensitive information with care, ensuring they are stored securely or disposed of properly.

Department heads carry the additional responsibility of ensuring that their team members are aware of and compliant with this policy. T hey must also conduct regular reviews of access privileges and report any concerns related to information security.

5. Data Access and Control Procedures.

Access to confidential information within STP is governed by a role -based system to ensure that individuals only access the information necessary for their job function. Key aspects of this system include:

- Access permissions must be formally requested, approved by a supervisor, and recorded.
- When an individual changes roles or leaves the organization, access rights are reviewed and promptly modified or revoked.
- Information systems, databases, and shared drives are organized to prevent unauthorized cross-departmental access.
- Periodic audits are conducted to verify access controls and identify any irregul arities or potential risks.

6. Security Measures and Technical Controls.

STP employs a combination of physical, administrative, and technological measures to protect sensitive data. These include:

- Encryption of files and communications to prevent unauth orized interception.
- Use of secure, password -protected systems and devices.
- Mandatory two -factor authentication for key platforms and databases.
- Regular software updates, antivirus installations, and firewall configurations.
- Restricted access to physical o ffices, files, and storage spaces containing sensitive records.
- Backup systems and disaster recovery protocols to safeguard against data loss.

All employees are expected to adhere strictly to IT security policies and to use only approved platforms for communication and data storage.

7. Data Disclosure and Third -Party Agreements.

Confidential information must not be shared with any external party unless there is a legitimate operational, legal, or contractual justification for doing so. In such cases, the following conditions must be met:

- Written authorization must be obtained from the Executive Director or delegated authority.
- A confidentiality or non -disclosure agreement must be signed by the receiving party.
- The receiving party's data protection and information security practices must be assessed.
- Data should be anonymized or encrypted when appropriate, especially when transferred electronically.
- Only secure communication channels (such as encrypted email or secure file transfer services) should be us ed.

STP ensures that all vendor, donor, and partner agreements contain confidentiality clauses that align with this policy.

8. Breach Identification and Response.

A breach of confidentiality occurs when unauthorized persons gain access to, or are exposed to, sensitive information. All breaches or suspected breaches must be reported immediately to the Data Protection Officer or designated senior manager.

Upon report, STP will take the following steps:

1. Contain and limit the exposure by isolating affected systems or files.
2. Investigate the source, scope, and impact of the breach.
3. Notify affected individuals, stakeholders, or authorities as required.
4. Document the incident and apply disciplinary or legal action where necessary.
5. Review the incident and revise security measures to prevent recurrence.

STP maintains a formal log of all breaches, including details of the incident and the remedial steps taken.

9. Training and Awareness.

Training and awareness are critical for ensuring compliance with this policy. To this end, STP conducts:

- Mandatory confidentiality training for all new employees and volunteers during onboarding.
- Annual refresher courses and targeted briefings for staff handling particularly sensitive information.
- Awareness campaigns through posters , emails, and internal meetings.
- Departmental training sessions tailored to specific roles or risks.

All staff are encouraged to stay informed and take ownership of their responsibility to protect STP's data assets.

10. Review, Compliance, and Enforcemen t.

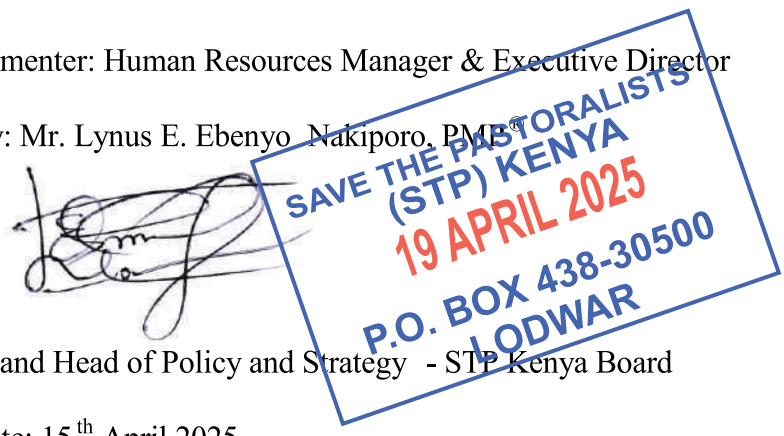
This policy is subject to annual review by the Human Resources and Compliance Teams or sooner in response to significant organizational or legal changes. All updates will be approved by the Executive Director and circulated to staff.

Violations of this policy may result in disciplinary actions, including verbal or written warnings, suspension, termination of employment or contracts, and possible legal consequences.

STP expects full cooperation from all individuals during investigations related to breache s of confidentiality. Everyone must sign a formal acknowledgment of understanding and acceptance of this policy upon employment or partnership initiation.

Policy Implementer: Human Resources Manager & Executive Director

Approved by: Mr. Lynus E. Ebenyo Nakiporo, PMP



Chairperson and Head of Policy and Strategy - STP Kenya Board

Approval Date: 15th April 2025

Next Review Date: 15 Th May 2026.