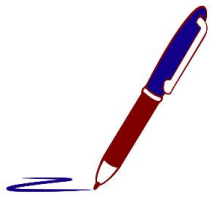

PEOPLE'S FORUM FOR REBUILDING DEMOCRACY (PFRD)

Address: The Spur Mall, 2nd Floor, Room 023, Thika Road,
P.O. Box 26181, Ruiru, Central, Kenya, 00100
Phone: +254 711 322 291
Email: info@pfrd.org

DATA PROTECTION AND PRIVACY POLICY

1. INTRODUCTION

The People's Forum for Rebuilding Democracy (PFRD) recognizes the right to privacy as a fundamental human right enshrined under Article 31 of the Constitution of Kenya, 2010. In line with the **Data Protection Act, 2019**, this policy establishes the framework within which PFRD collects, processes, stores, shares, and protects personal data of its members, employees, volunteers, partners, and the public.

PFRD is committed to maintaining the **highest standards of confidentiality, transparency, and accountability** in all its data management practices.

2. PURPOSE AND OBJECTIVES

The purpose of this policy is to:

1. Ensure compliance with the **Data Protection Act, 2019**, and relevant subsidiary legislation.
2. Establish clear principles and responsibilities for the management of personal data within PFRD.
3. Safeguard personal data against unauthorized access, loss, disclosure, alteration, or destruction.

4. Promote trust among members, partners, and the public by ensuring that data is handled lawfully and ethically.

3. SCOPE

This policy applies to:

- All PFRD members, officials, and employees.
- Contractors, consultants, and volunteers engaged by PFRD.
- All third parties handling personal data on behalf of PFRD.
- All personal data collected through membership forms, online platforms, social media, communications, surveys, and public engagements.

4. LEGAL AND REGULATORY FRAMEWORK

This policy is guided by the following laws and frameworks:

- The **Constitution of Kenya, 2010** (Article 31 – Right to Privacy)
- The **Data Protection Act, 2019** and associated Regulations
- The **Political Parties Act, 2011** (as amended)
- The **Public Service (Values and Principles) Act, 2015**
- The **Access to Information Act, 2016**
- Other applicable laws and international best practices on data management

5. DEFINITIONS

- **Personal Data:** Information relating to an identified or identifiable natural person.
- **Sensitive Personal Data:** Includes details such as race, ethnic origin, political opinions, religious beliefs, biometric data, or health information.
- **Data Subject:** The individual whose personal data is being processed.
- **Data Controller:** The person or entity that determines the purpose and means of processing personal data (PFRD in this case).
- **Data Processor:** A person or entity that processes personal data on behalf of the controller.
- **Processing:** Any operation performed on personal data, such as collection, recording, storage, adaptation, retrieval, or dissemination.

6. PRINCIPLES OF DATA PROTECTION

PFRD adheres to the following data protection principles:

1. **Lawfulness, Fairness, and Transparency** – Data will be processed lawfully and fairly, with clear communication to the data subject.
2. **Purpose Limitation** – Data shall only be collected for specific, explicit, and legitimate purposes.
3. **Data Minimization** – Only data necessary for the intended purpose shall be collected.
4. **Accuracy** – Data shall be kept accurate and up to date.
5. **Storage Limitation** – Data shall not be kept longer than necessary.
6. **Integrity and Confidentiality** – Appropriate security measures shall protect data from unauthorized access or misuse.
7. **Accountability** – PFRD shall be responsible for demonstrating compliance with all principles of data protection.

7. TYPES OF PERSONAL DATA COLLECTED

PFRD may collect the following categories of personal data:

- Member registration details (names, ID/passport numbers, gender, age, contact information, constituency, ward, etc.)
- Employee and volunteer details (CVs, employment records, bank details, emergency contacts, etc.)
- Political participation data (membership activity, attendance records, leadership roles)
- Communication records (emails, letters, feedback forms)
- Digital engagement data (social media interactions, website analytics)

Sensitive data, such as political affiliations or biometric data, will only be processed with the **explicit consent** of the data subject.

8. DATA COLLECTION AND CONSENT

1. Personal data shall be collected directly from the data subject, except where lawful exceptions apply.

2. Consent shall be obtained before data collection and may be withdrawn at any time.
3. For minors (under 18 years), consent shall be obtained from a parent or legal guardian.
4. Data subjects shall be informed of:
    - The purpose of data collection.
    - The use of their data.
    - Their rights to access, correct, or delete their data.

9. DATA STORAGE AND SECURITY

1. Personal data shall be stored in secure physical and electronic formats, including locked filing systems and password-protected databases.
2. Access to personal data shall be restricted to authorized personnel only.
3. PFRD shall use encryption, firewalls, and antivirus protection for digital records.
4. Regular data security audits and risk assessments shall be conducted to ensure compliance and protection against data breaches.

10. DATA SHARING AND DISCLOSURE

1. PFRD shall not disclose personal data to third parties except:
    - With the consent of the data subject;
    - Where required by law or court order; or
    - To service providers contracted to deliver legitimate party services (e.g., ICT hosting or voter outreach).
2. All third-party processors shall sign confidentiality and data protection agreements with PFRD.

---

11. DATA RETENTION AND DISPOSAL

1. Personal data shall only be retained for as long as necessary for the purposes collected or as required by law.
2. When data is no longer required, it shall be securely deleted or destroyed using approved methods (e.g., shredding, digital wiping).

3. PFRD shall maintain a **Data Retention Schedule** defining specific retention periods for various data categories.

12. RIGHTS OF DATA SUBJECTS

Every data subject has the following rights:

1. To be informed of the processing of their personal data.
2. To access their personal data held by PFRD.
3. To request correction or deletion of inaccurate or outdated data.
4. To withdraw consent for processing.
5. To object to data processing on legitimate grounds.
6. To lodge a complaint with the **Office of the Data Protection Commissioner (ODPC)** if aggrieved.

13. DATA BREACH MANAGEMENT

1. In case of a data breach, PFRD shall:
    - Contain the breach immediately.
    - Notify affected individuals within 72 hours of detection.
    - Report the breach to the ODPC as required by law.
    - Investigate the incident and take corrective measures.
2. Records of all breaches and responses shall be maintained for accountability.

14. TRAINING AND AWARENESS

PFRD shall ensure continuous training of staff, members, and volunteers on:

- Data protection principles;
- Cybersecurity best practices; and
- Procedures for reporting and managing data breaches.

15. IMPLEMENTATION AND COMPLIANCE

The **Secretary-General** of PFRD shall be responsible for the implementation of this policy, supported by a **Data Protection Officer (DPO)** who will:

- Oversee compliance with the Data Protection Act;

- Conduct audits;
- Serve as the contact person for the ODPC and data subjects; and
- Report annually to the National Executive Committee on compliance status.

16. REVIEW AND AMENDMENT

This policy shall be reviewed every two years or sooner if:

- There are amendments to the Data Protection Act;
- The ODPC issues new guidelines; or
- There is a significant change in PFRD's data handling processes.

All revisions shall be approved by the **National Executive Council (NEC)** of PFRD.

17. POLICY APPROVAL

Signed:

_____

Party Leader / National Chairperson

People's Forum for Rebuilding Democracy (PFRD)

_____

Secretary-General

People's Forum for Rebuilding Democracy (PFRD)