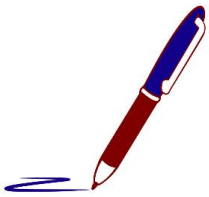

People's Forum for Rebuilding Democracy (PFRD)

Address:
The Spur Mall – 2nd Floor, Room 023
Thika Road,
P.O Box 26181, Ruiru – Central, Kenya, 00100
Email: info@pfrd.org | **Phone:** +254 711 322 291
Website: www.pfrd.org *(if applicable)*

Policy Title:

ICT (Information & Communications Technology) Policy

1. Introduction

The People's Forum for Rebuilding Democracy (PFRD) recognizes Information and Communications Technology (ICT) as a critical enabler in advancing democratic governance, transparency, party coordination, and member engagement. This policy provides a framework to ensure secure, lawful, reliable, and ethical use of PFRD's ICT infrastructure and digital assets in alignment with its political, administrative, and operational objectives.

The policy safeguards party data, personal information of members, and the integrity of political communication and engagement in accordance with Kenyan law.

1.1 Purpose

The purpose of this policy is to:

- Protect PFRD's ICT resources from misuse, damage, or compromise.
- Ensure confidentiality, integrity, and availability of party data and systems.
- Comply with the *Data Protection Act, 2019* and related laws.
- Establish clear responsibilities and procedures for ICT management and usage.
- Promote transparency, accountability, and digital security in party operations.

1.2 Scope

This policy applies to:

- All PFRD officials, elected representatives, staff, volunteers, consultants, and contractors.
- All PFRD offices — national headquarters, county, constituency, and ward offices.
- Any person or entity accessing, managing, or using PFRD ICT systems, whether on-site or remotely.

It covers the use of:

- Computers, mobile devices, and tablets.
- Party networks, Wi-Fi, and internet services.
- Party-managed websites, databases, and cloud services.
- Email, social media, and communication platforms.
- Electronic data storage and transmission systems.

1.3 Definitions

- **ICT Resources:** All electronic systems, devices, networks, and digital services owned or leased by PFRD.
- **Personal Data:** Information relating to an identifiable natural person as defined under the *Data Protection Act, 2019*.
- **Sensitive Party Information:** Internal records such as strategy documents, membership registers, donor lists, financial records, and confidential minutes.

- **Data Breach:** Unauthorized access, disclosure, alteration, or destruction of data.
- **Users:** Any authorized individual accessing PFRD ICT systems.

1.4 Principles

This policy is guided by the following principles:

1. **Lawfulness:** All ICT activities must comply with Kenyan laws and regulations, including:
    - *Computer Misuse and Cybercrimes Act, 2018*
    - *Data Protection Act, 2019*
    - *Political Parties Act, 2011*
    - *Public Officer Ethics Act, 2003*
    - *Constitution of Kenya, 2010*
2. **Confidentiality:** Party data must be protected from unauthorized access or disclosure.
3. **Integrity:** Data must remain accurate and unaltered except by authorized persons.
4. **Availability:** Systems and data must be accessible to authorized users when needed.
5. **Transparency:** Members must be informed of how their data is collected, used, and stored.
6. **Accountability:** Every user is responsible for ethical and lawful use of ICT resources.

1.5 Acceptable Use

- ICT systems shall be used solely for **official party business** and not for personal commercial or illegal activities.
- Limited personal use may be permitted where it does not compromise system performance or security.
- Prohibited activities include:
    - Hacking or unauthorized access.

- Distribution of malicious software (malware).
- Unauthorized political advertising, fake news, or impersonation.
- Cyber harassment or defamation.
- Transmission of discriminatory or offensive content.
- Mass unsolicited messaging without consent (in breach of the *Data Protection Act*).

1.6 Access Control & Authentication

- All users shall be assigned **unique usernames and passwords**.
- **Multi-Factor Authentication (MFA)** is mandatory for system administrators and remote logins.
- Access rights will be role-based (RBAC) and aligned with official responsibilities.
- Passwords must meet minimum security standards:
  - At least 10 characters, including letters, numbers, and symbols.
  - Changed every 90 days.
  - Never shared or written down insecurely.

1.7 Data Classification & Handling

All PFRD data must be classified and handled appropriately:

- **Public:** Information available for public dissemination (e.g., press releases).
- **Internal:** Non-sensitive administrative data.
- **Restricted:** Operational data with limited access.
- **Confidential:** Sensitive records (membership, finances, strategy).

Data handling must include:

- Encryption in storage and transmission.
- Secure deletion of outdated data.
- Controlled data sharing with third parties (only under NDA and with NEC approval).

1.8 Data Protection & Privacy

PFRD commits to full compliance with the *Data Protection Act, 2019*.

- Personal data will be collected and processed lawfully and fairly.
- Data will only be used for legitimate party purposes (e.g., membership management).
- Consent shall be obtained from members before collecting personal details.
- Data subjects have rights to:
    - Access their data.
    - Request correction or deletion.
    - Withdraw consent.
    - Lodge complaints with the **Office of the Data Protection Commissioner (ODPC)**.

The **Data Protection Officer (DPO)** shall oversee compliance and handle all related inquiries.

1.9 Incident Response & Reporting

All ICT incidents (security breach, hacking attempt, data loss) must be reported immediately to the **ICT Officer** and **DPO**.

An **Incident Response Plan (IRP)** shall include:

- Containment and isolation of affected systems.
- Eradication of malware or intruders.
- System recovery and service restoration.
- Notification of affected members (and ODPC if required).
- Post-incident review and policy improvement.

1.10 Email & Communication

- Official communication must use **PFRD domain emails** (e.g., *@pfrd.org*).

- Personal email accounts shall not be used for party business.
- Phishing awareness training is mandatory.
- Confidential documents must not be sent to unauthorized recipients.

1.11 Social Media & Online Presence

- Only designated communication officers may post on official accounts.
- Posts must reflect verified party positions, be factual, and avoid hate speech.
- Unauthorized individuals are prohibited from creating or managing party-related pages or groups.
- Defamatory or inciteful content will attract disciplinary action.

1.12 Software, Licensing & Updates

- Only licensed software shall be installed on PFRD systems.
- Pirated or unlicensed software is strictly prohibited.
- ICT department shall ensure regular system updates and patching.

1.13 Remote Work & BYOD (Bring Your Own Device)

- Staff working remotely must connect through **secure VPN** with MFA.
- Personal devices must be enrolled under PFRD's BYOD policy with anti-malware and encryption.
- No confidential data shall be stored on personal devices without authorization.

1.14 Backups & Business Continuity

- Regular, encrypted backups must be performed weekly and stored securely (onsite and offsite).
- The ICT team shall maintain a **Business Continuity and Disaster Recovery Plan (BCP/DRP)**.

- Periodic simulations shall be conducted to test recovery procedures.

1.15 Monitoring & Privacy

- PFRD may monitor ICT usage to protect systems and data integrity.
- Monitoring will be limited, documented, and consistent with privacy rights under Kenyan law.
- Users will be notified where monitoring is implemented.

1.16 Roles & Responsibilities

Role	Responsibility
National Executive Committee (NEC)	Approves ICT policy, allocates budget, provides oversight.
ICT Officer	Implements policy, manages systems, ensures security and training.
Data Protection Officer (DPO)	Ensures compliance with Data Protection Act; reports breaches.
Party Members & Staff	Follow ICT usage rules; report suspicious activities.
County/Branch ICT Coordinators	Oversee local ICT operations and report to National ICT Officer.

1.17 Training & Awareness

- Mandatory induction training on ICT use, cybersecurity, and data privacy for all new staff and volunteers.
- Annual refresher courses for all party officials.
- Periodic workshops on digital communication ethics and online safety.

1.18 Disciplinary Measures

Any breach of this policy may result in:

- Warning or suspension of ICT access.
- Disciplinary action under PFRD HR policy.
- Reporting to authorities for criminal acts (e.g., cybercrime).
- Legal action and potential civil penalties.

1.19 Policy Review

This policy shall be reviewed annually by the ICT Officer and DPO, and approved by the NEC. Revisions may also occur after major incidents, technological changes, or amendments to Kenyan ICT or data laws.

Signed:

_____

Party Leader / National Chairperson

People's Forum for Rebuilding Democracy (PFRD)

_____

Secretary-General

People's Forum for Rebuilding Democracy (PFRD)