UFORO MICROFINANCE BANK LIMITED

NO 4 MARKET ROAD, IKPE IKOT NKON, INI LGA, AKWA IBOM STATE

DATA PRIVACY AND PROTECTION POLICY

TABLE OF CONTENT

Chapter One

Chapter Two

Chapter One

1.0 DATA PRIVACY AND PROTECTION OVERVIEW

1.1 Introduction

Uforo Microfinance Bank Ltd ("Uforo MFB" or "the Bank") is committed to protecting the privacy and personal data of its customers, employees, shareholders, vendors, and other stakeholders. This Data Privacy and Protection Policy outlines how the Bank collects, uses, stores, discloses, and protects personal data in compliance with applicable laws and regulatory requirements, including the Nigeria Data Protection Act (NDPA) 2023 and relevant Central Bank of Nigeria (CBN) guidelines.

1.1 Objectives of the Policy

The objectives of this policy are to: -

1. Ensure that personal data is processed lawfully, fairly, and transparently.
2. Safeguard personal data against unauthorized access, loss, misuse, alteration, or destruction.
3. Promote a culture of data privacy and confidentiality within the Bank. Define responsibilities for data protection and privacy compliance.
4. Ensure compliance with applicable data protection laws and regulations.

1.2 Scope

This policy applies to:

1. All employees, directors, management, contract staff, and agents of Uforo MFB.
2. All personal data processed by the Bank, whether in electronic, paper, or other forms.
3. All data subjects, including customers, prospective customers, staff, vendors, and other stakeholders.

1.3 Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person.

- **Data Subject**: An individual whose personal data is processed by the Bank.
- **Processing**: Any operation performed on personal data, including collection, storage, use, disclosure, or deletion.
- **Data Controller**: Uforo Microfinance Bank Ltd, which determines the purpose and means of processing personal data.
- **Data Processor**: Any third party that processes personal data on behalf of the Bank.

1.4 Legal and Regulatory Framework

This policy is guided by, but not limited to, the following: - Nigeria Data Protection Act (NDPA) 2023 - Nigeria Data Protection Regulation (NDPR) 2019 - Central Bank of Nigeria (CBN) Consumer Protection Framework - BOFIA 2020 (as amended) - Other applicable laws and regulatory guidelines

---

1.5 Principles of Data Protection

Uforo MFB shall adhere to the following data protection principles:

1. Lawfulness, Fairness, and Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

1.6 Lawful Basis for Processing

The Bank shall process personal data only where at least one of the following applies: -

1. Consent of the data subject.
2. Performance of a contract.
3. Compliance with legal or regulatory obligations.
4. Protection of vital interests of the data subject.

5. Performance of a task carried out in the public interest.
6. Legitimate interests of the Bank, provided such interests do not override the rights of the data subject

---

1.7 Collection and Use of Personal Data

The Bank may collect personal data for purposes including but not limited to:

1. Account opening and customer onboarding (KYC).
2. Credit appraisal and loan management.
3. Employment and human resource administration.
4. Regulatory reporting and compliance - Service delivery and customer relationship management

Personal data shall only be used for the purposes for which it was collected, unless otherwise required by law.

1.8 Data Security Measures

Uforo MFB shall implement appropriate technical and organizational measures to protect personal data, including:

1. Access controls and authentication mechanisms.
2. Encryption and secure storage systems.
3. Physical security of records and IT infrastructure.
4. Regular system updates and security monitoring.
5. Staff training and confidentiality agreements

1.9 Data Sharing and Disclosure

Personal data may be shared with: -

1. Regulatory authorities such as the CBN, NDPC, and other lawful agencies.
2. Service providers and vendors under contractual confidentiality obligations.
3. Credit bureaus and payment service providers, where applicable

The Bank shall not disclose personal data to unauthorized third parties.

1.10 Rights of Data Subjects

Data subjects have the right to: -

1. Access their personal data.
2. Request correction or update of inaccurate data.
3. Withdraw consent (where applicable).
4. Request deletion or restriction of processing, subject to legal obligations.
5. Lodge complaints with the Nigeria Data Protection Commission (NDPC).

1.11 Data Retention and Disposal

Personal data shall be retained only for as long as necessary to fulfill the purpose for which it was collected or as required by law. Upon expiration of the retention period, data shall be securely destroyed or anonymized.

1.12 Data Breach Management

In the event of a data breach, the Bank shall: -

1. Promptly assess the nature and impact of the breach.
2. Take immediate steps to contain and remedy the breach.
3. Notify relevant regulatory authorities and affected data subjects where required by law.
4. Document and review the incident to prevent recurrence

1.13 Roles and Responsibilities

- **Board of Directors**: Oversight of data protection governance
- **Management**: Implementation and enforcement of this policy
- **Data Protection Officer (DPO)**: Monitoring compliance and advising on data protection matters
- **Employees**: Compliance with this policy and confidentiality obligations

1.14 Training and Awareness

The Bank shall provide regular data privacy and protection training to employees to ensure awareness and compliance with this policy.

1.15 Policy Review and Updates

This policy shall be reviewed periodically or as required by changes in laws, regulations, or the Bank's operations.

1.16. References

- Nigeria Data Protection Act (NDPA 2023)
- Nigeria Data Protection Regulation (NDPR)
- ISO/IEC 27001: Information Security Management Standard
- Organization's Internal Policies and SOPs.

CHAPTER TWO

2.0 DATA BREACH RESPONSE STANDARD OPERATING PROCEDURE (SOP)

2.1 PURPOSE

This Standard Operating Procedure (SOP) provides a lawful, timely, and risk-based framework for managing personal data breaches at Uforo Microfinance Bank (MFB), fully aligned with the Nigeria Data Protection Act (NDPA) 2023. It aims to safeguard the rights and freedoms of data subjects, ensure regulatory compliance, promote accountability, and strengthen operational resilience.

2.2 LEGAL AND REGULATORY BASIS

This SOP is issued pursuant to:

- Nigeria Data Protection Act (NDPA) 2023
- Nigeria Data Protection Commission (NDPC) Guidelines and Directives
- Central Bank of Nigeria (CBN) Data Protection and Consumer Protection Frameworks

Where conflicts arise, the NDPA 2023 shall prevail.

2.3 SCOPE

This SOP applies to:

- All personal data processed by Uforo MFB (customers, staff, directors, vendors, and third parties)
- All processing activities (collection, storage, transmission, deletion)
- All employees, contract staff, agents, and data processors acting on behalf of the Bank
- All systems: electronic, manual, cloud-based, and physical records

2.4 DEFINITIONS (NDPA-BASED)

- **Personal Data:** Any information relating to an identified or identifiable natural person, as defined under the NDPA 2023.
- **Sensitive Personal Data:** Includes financial information, biometric data, BVN, NIN, authentication credentials, and any data requiring enhanced protection.
- **Personal Data Breach:** A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
- **Data Controller:** Uforo Microfinance Bank (MFB).

- **Data Processor:** Any third party processing personal data on behalf of the Bank.
- **Nigeria Data Protection Commission (NDPC):** The statutory authority established under the NDPA 2023.

2.5 GOVERNANCE, ACCOUNTABILITY, AND ROLES

2.5.1 Board of Directors

- Ensure oversight and accountability for data protection governance
- Approve notifications involving high-risk or systemic breaches

2.5.2 Managing Director / CEO

- Ensure institutional compliance with NDPA obligations
- Authorize breach notifications to the NDPC and affected data subjects

2.5.3 Data Protection Officer (DPO)

- Act as the primary coordinator for breach response
- Conduct risk assessments in line with NDPA Section on breach notification
- Liaise with the NDPC and other regulators
- Maintain the Personal Data Breach Register

2.5.4 Information Technology / Information Security Unit

- Detect, analyze, contain, and remediate breaches
- Preserve forensic evidence and logs
- Implement corrective technical measures

2.5.5 Legal & Compliance Unit

- Interpret statutory obligations and timelines under NDPA
- Advise Management on legal exposure and enforcement risks

2.5.6 Employees and Contractors

- Report suspected or actual data breaches immediately
- Comply with confidentiality and incident response directives

2.6 IDENTIFICATION OF A PERSONAL DATA BREACH

A personal data breach may be identified through:

- Security monitoring systems

- Staff reports or whistleblowing
- Customer complaints
- Third-party or processor notifications
- Internal or external audits

Indicators include unauthorized access, data leakage, ransom ware, phishing incidents, or loss of devices containing personal data.

2.7 IMMEDIATE REPORTING REQUIREMENTS

1. Any employee or processor who becomes aware of a suspected breach **must report immediately and not later than 1 hour** to the DPO.
2. The report shall contain:
    - Date and time of discovery
    - Nature and circumstances of the breach
    - Categories of personal data involved
    - Systems, processes, or persons affected
    - Immediate containment actions taken

Failure to report promptly constitutes a breach of duty under NDPA accountability principles.

2.8 RISK ASSESSMENT (NDPA COMPLIANCE TEST)

The DPO shall assess whether the breach is likely to result in:

- Risk to the rights and freedoms of data subjects, or
- High risk requiring mandatory notification

Assessment factors include:

- Type and sensitivity of personal data
- Volume of data affected
- Ease of identification of data subjects
- Potential financial, identity, or reputational harm

2.9 CONTAINMENT AND MITIGATION

Upon confirmation of a breach, the Bank shall without delay:

- Isolate affected systems
- Revoke or suspend compromised access
- Secure backups and logs

- Prevent further unauthorized processing

All containment measures shall be documented for regulatory accountability.

2.10 NOTIFICATION OBLIGATIONS UNDER NDPA 2023

10.1 Notification to the Nigeria Data Protection Commission (NDPC)

Where a breach is likely to result in risk to data subjects, Uforo MFB shall notify the NDPC **without undue delay** and in line with NDPC-issued timelines, providing:

- Description of the breach
- Categories and approximate number of data subjects affected
- Likely consequences of the breach
- Measures taken or proposed to address the breach

10.2 Notification to Data Subjects

Where the breach is likely to result in **high risk** to data subjects, the Bank shall notify affected individuals clearly and promptly, stating:

- Nature of the breach
- Personal data affected
- Protective steps taken by the Bank
- Recommended actions for data subjects

2.11. INVESTIGATION AND ROOT CAUSE ANALYSIS

The Incident Response Team shall:

- Conduct forensic investigation
- Identify control weaknesses and compliance failures
- Document findings and corrective actions

2.12. RECOVERY AND REMEDIATION

- Restore systems securely
- Strengthen administrative, technical, and organizational safeguards
- Review data processing agreements with processors
- Conduct targeted staff retraining

2.13. RECORD KEEPING AND BREACH REGISTER

In compliance with NDPA accountability requirements, the DPO shall maintain a **Personal Data Breach Register** containing:

- Facts relating to the breach
- Effects and impact assessment
- Remedial actions taken

Records shall be retained for **a minimum of six (6) years** and made available to the NDPC upon request.

2.14. DISCIPLINARY AND ENFORCEMENT MEASURES

Non-compliance with this SOP, negligence, or willful misconduct relating to personal data breaches shall attract disciplinary action in line with the Bank's HR policies and applicable laws.

2.15. TRAINING AND AWARENESS

- Mandatory annual NDPA-focused data protection training
- Periodic breach simulations and tabletop exercises

2.16. REVIEW AND CONTINUOUS IMPROVEMENT

This SOP shall be reviewed:

- Annually
- Upon any amendments to the NDPA or NDPC directives
- After any significant personal data breach

CHATPTER THREE

3.0 DATA SUBJECT ACCESS REQUEST (DSAR) PROCEDURE

3.1 Purpose

This procedure defines the Bank's process for handling Data Subject Access Requests (DSARs) in line with the Nigeria Data Protection Act (NDPA) 2023, the Bank's Data Privacy & Protection Policy, and the Data Breach Response SOP. It ensures that all DSARs are received, verified, processed, and responded to in a transparent, accountable, and secure manner, protecting data subject rights and preventing unauthorized disclosure or data breaches.

3.2 Scope

This procedure applies to all DSARs received from individuals (customers, employees, former employees, vendors, agents, and other identifiable persons) whose personal data are processed by the Bank, across all processing activities, systems, records, and third-party processors.

3.3 Legal Basis

- Nigeria Data Protection Act (NDPA) 2023
- NDPC Regulations, Codes of Conduct, and Guidelines (as applicable)
- Applicable sectorial regulations (e.g., CBN requirements), where consistent with NDPA

3.4 Definitions

- **Data Subject**: An identifiable natural person whose personal data are processed.
- **DSAR**: A request by a data subject to exercise rights over personal data (access, rectification, erasure, restriction, portability, objection, or withdrawal of consent).
- **Personal Data**: Any information relating to an identified or identifiable natural person.
- **Sensitive Personal Data**: As defined by NDPA 2023.
- **Controller**: The Bank, determining purposes and means of processing.
- **Processor**: Any third party processing personal data on behalf of the Bank.
- **DPO**: Data Protection Officer.

3.5 Data Subject Rights Covered

Under the NDPA 2023, data subjects may request to:

- Access their personal data
- Rectify inaccurate or incomplete data
- Erase personal data (right to be forgotten)
- Restrict processing
- Object to processing
- Data portability (where applicable)
- Withdraw consent (where processing is consent-based)

3.6 Roles and Responsibilities

6.1 Board and Management

- To provide oversight and resources for DSAR compliance.

6.2 Data Protection Officer (DPO)

- Serve as the primary point of contact for DSARs.
- Ensure lawful, timely, and accurate responses.
- Maintain DSAR records and reports.
- Liaise with NDPC where required.

6.3 Compliance / Legal Unit

- Advise on exemptions, refusals, and redactions.
- Review complex or high-risk DSARs.

6.4 IT / Operations

- Identify, retrieve, and securely extract requested data.
- Support redaction and secure delivery.

6.5 All Staff

- Promptly forward any DSAR received to the DPO.

3.7 Channels for Submitting DSARs

DSARs may be submitted through:

- Written request (letter)
- Email to the designated data protection address
- Bank-approved DSAR form (physical or electronic)
- In-person request (documented by staff)

Anonymous or unverifiable requests will not be processed.

3.8 DSAR Handling Procedure

Step 1: Receipt and Logging

- All DSARs must be forwarded to the DPO within 24 hours of receipt.
- The DPO logs the request in the DSAR Register, capturing:
  - Date received
  - Requester identity
  - Nature of request
  - Reference number

Step 2: Acknowledgement

- Acknowledge receipt to the data subject within **7 days**.
- Inform the data subject of timelines and verification requirements.

Step 3: Identity Verification

- Verify the requester's identity using reasonable and proportionate measures.
- Where a representative acts on behalf of a data subject, require written authorization.
- Processing does not commence until verification is complete.

Step 4: Request Assessment

- Determine the scope and type of request.
- Assess applicability of NDPA rights and any lawful exemptions.
- Identify systems, departments, and processors involved.

Step 5: Data Retrieval and Review

- Retrieve relevant personal data securely.
- Review for accuracy, relevance, and third-party data.
- Apply redactions where disclosure would adversely affect the rights of others or fall under lawful exemptions.

Step 6: Response Preparation

- Compile the response in clear, plain language.
- Include:
  - Confirmation of whether personal data are processed
  - Categories of data
  - Purposes of processing

- Data sources
- Recipients or categories of recipients
- Retention periods
- Rights available to the data subject

Step 7: Response Delivery

- Provide the response within **30 days** of receipt of a valid request, as required by NDPA 2023.
- Where requests are complex or numerous, extend once (with justification) and notify the data subject promptly.
- Deliver responses securely (encrypted email, secure portal, or sealed hard copy).

3.9 Fees

- DSARs are processed **free of charge**.
- A reasonable administrative fee may apply only where requests are manifestly unfounded, excessive, or repetitive, in line with NDPA guidance.

3.10 Refusal or Limitation of Requests

A DSAR may be refused or limited where:

- Disclosure would prejudice national security, public interest, crime prevention, or regulatory functions.
- It would infringe the rights and freedoms of others.
- The request is manifestly unfounded or abusive.

Any refusal must:

- Be approved by the DPO and Legal/Compliance.
- Be communicated in writing, stating reasons and available remedies.

3.11 Third-Party Processors

- Where data are processed by third parties, the DPO shall coordinate timely retrieval.
- Processors must support DSARs under contractual obligations.

3.12 Record Keeping and Audit

- Maintain a DSAR Register and supporting documentation for a minimum period prescribed by NDPA and internal policy.

- DSAR records shall be available for NDPC inspection.

3.13 Training and Awareness

- All staff shall receive periodic training on recognizing and escalating DSARs.

3.14 Breach Escalation and Policy Integration

- DSAR handling shall strictly comply with the Bank's **Data Privacy & Protection Policy**, including principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.
- Any suspected or actual unauthorized access, disclosure, loss, or misuse of personal data identified during DSAR processing shall be treated as a **data breach** and escalated immediately in line with the Bank's **Data Breach Response SOP**.
- The DPO shall coordinate containment, assessment, notification, and documentation of such incidents in accordance with NDPA 2023 and NDPC reporting timelines.
- DSAR responses shall be suspended where necessary to prevent further risk until breach containment measures are implemented.

CHAPTER FOUR

4.0 CUSTOMER PRIVACY NOTICE WITH OPERATIONAL CONTROLS

4.1 Introduction

The Bank is committed to protecting customer's personal data and ensuring that privacy is respected. This notice outlines not only how we collect, use, and share customer's information, but also the operational controls that govern these processes.

4.2. Categories of Personal Data Collected & Operational Controls

Data Type	Purpose	Operational Control / Workflow
Identity & Contact (Name, DOB, Address, Email, Phone)	Customer onboarding, communication, service delivery	Collected via secured forms; verified against ID; stored in encrypted CRM accessible only to authorized staff
Identification Documents (ID, Passport, Driver's License)	Identity verification, regulatory compliance (KYC/AML)	Uploaded to secure server; access restricted to compliance team; logged for audit; destroyed after retention period (**Must be approved**).
Financial & Transaction Data	Account management, payments, fraud detection	Stored in encrypted core banking system; access role-based; monitored with audit logs; transactions flagged for anomalies
Usage & Interaction Data (Online activity, app usage)	Service improvement, analytics, marketing	Collected via secure web/app interfaces; anonymized for analytics where possible; access restricted to IT & analytics teams
Communications (calls, emails, chats)	Customer support, dispute resolution	Stored in secure repository; access restricted to support staff; monitored for quality assurance

4.3 Data Processing Purpose & Legal Basis

Purpose	Legal / Regulatory Basis	Operational Implementation
Service provision & account management	Contractual necessity	Automated workflows in CRM/Core Banking; activity logs maintained
Identity verification &	Regulatory requirement	Compliance team performs KYC

Purpose	Legal / Regulatory Basis	Operational Implementation
fraud prevention	(NDPA, CBN guidelines)	checks; verification logs retained; periodic review
Regulatory reporting & audits	Legal obligation	Data exported under secure channels; access logged; reports stored securely
Customer communication & marketing	Consent / legitimate interest	Opt-in consent recorded; unsubscribe options available; marketing logs audited
Risk, audit, compliance	Legal & operational necessity	Internal audit teams have role-based access; regular reporting to DPO

4.4 Data Sharing & Operational Controls

Shared With	Purpose	Controls
Internal Departments	Service delivery, dispute resolution	Need-to-know access; role-based permissions; activity logging
Third-party Vendors	IT services, payment processing	Contractual NDA; limited access; audit rights; data anonymization where possible
Regulatory Authorities	Legal compliance & reporting	Secure transmission channels; formal request validation; audit trail maintained
With Customer Consent	Marketing, promotional campaigns	Explicit opt-in; consent logs; withdrawal mechanism implemented

4.5 Data Retention & Disposal Workflow

Data Type	Retention Period	Operational Disposal Method
Customer onboarding documents	5–7 years (or per regulatory guideline)	Shredding (physical), secure deletion (digital)
Transaction records	Minimum regulatory period (e.g., 7 years)	Archived in secure storage; encrypted; access limited
Marketing & communications data	Until consent withdrawn	Soft delete in CRM; permanently deleted after opt-out + retention period
Logs & Audit trails	5 years	Encrypted storage; access logs; deleted per schedule

4.6 Customer Rights & Staff Operational Actions

Customer Right	Staff Action / Operational Control
Access	Verify identity, retrieve requested data from secured system, log request
Correction	Update CRM / core banking records; maintain change logs
Deletion / Restriction	Flag data for deletion or restriction; coordinate with IT for secure removal
Consent Withdrawal	Update marketing preference in system; confirm with customer; log action
Data Portability	Extract requested data in standard format; provide securely; log provision
Complaint	Route to DPO; investigate; respond within regulatory timelines

4.7 Security Measures & Operational Controls

Control Area	Operational Implementation
Access Control	Role-based access; multi-factor authentication; regular review of user permissions
Encryption & Secure Storage	All personal data encrypted in transit & at rest; backups encrypted
Monitoring & Logging	System logs retained for audit; anomaly detection in transactions & data access
Staff Training	Mandatory privacy, security, and NDPA compliance training; annual refreshers
Incident Response	SOP for breach detection, reporting, containment, and notification; DPO oversight

4.8 Contact Information & Operational Support

- **Data Protection Officer (DPO):** [Insert Name]
- **Email:** [Insert Email]
- **Phone:** [Insert Phone Number]
- **Operational Support:** All requests and incidents are logged in the Privacy Management System and tracked for closure and audit purposes.

Chapter Five

5.0 GOVERNANCE AND REGULATORY COMPLIANCE ON DATA PROTECTION POLICY

5.1 Purpose

This policy establishes the framework for governance, management, and regulatory compliance regarding data protection within [Organization Name]. It ensures that all personal and sensitive data is collected, processed, stored, and disposed of in compliance with applicable laws and regulations, including but not limited to the **Nigeria Data Protection Act (NDPA 2023)**, **NDPR**, and international best practices.

5.2 Scope

This policy applies to:

- All employees, contractors, consultants, and third-party service providers of Uforo Microfinance Bank Limited.
- All personal data processed by the organization, whether in electronic or physical form.
- All systems, applications, and platforms used to process personal or sensitive data.

5.3 Governance Structure

3.1 Data Governance Committee

- Composed of senior management, legal, compliance, and IT representatives.
- Responsible for oversight of data protection policies, compliance programs, and risk management.
- Reviews and approves all data protection initiatives and audits.

3.2 Data Protection Officer (DPO)

- Appointed to ensure compliance with NDPA 2023 and other applicable regulations.
- Duties include:
  - Monitoring compliance with data protection policies.
  - Advising management on data protection impact assessments.
  - Acting as the contact point for the National Data Protection Bureau (NDPB) and data subjects.

3.3 Roles and Responsibilities

- **Employees:** Adhere to data protection principles and report breaches or risks.
- **IT Department:** Implement technical measures to protect data integrity, confidentiality, and availability.
- **Compliance/Legal:** Ensure organizational processes align with current laws and regulations.

5.4 Regulatory Compliance Framework

4.1 Legal Requirements

- Compliance with the **NDPA 2023**, NDPR, and other sector-specific regulations.
- Monitoring and adapting policies to reflect updates or new regulations.

4.2 Data Protection Principles

- Lawfulness, fairness, and transparency.
- Purpose limitation.
- Data minimization.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Accountability.

4.3 Documentation and Reporting

- Maintain a **Record of Processing Activities (RoPA)** for all personal data.
- Report data breaches to the relevant regulatory authority within the legally prescribed timeframes.
- Conduct regular audits to ensure compliance with policies and regulatory requirements.

5.5 Data Protection Controls

5.1 Organizational Controls

- Regular staff training on data protection and privacy obligations.
- Policies and SOPs governing access, processing, retention, and disposal of personal data.

5.2 Technical Controls

- Encryption of sensitive and personal data in transit and at rest.
- Secure authentication, access controls, and audit logging.
- Regular vulnerability assessments and penetration testing.

5.3 Third-Party Management

- Due diligence on third-party processors to ensure they comply with NDPA 2023 and contractual obligations.
- Data processing agreements (DPA) executed with all relevant third parties.

5.6 Monitoring, Audit, and Review

- Regular internal audits to assess compliance and identify gaps.
- Data Protection Impact Assessments (DPIA) for high-risk processing activities.
- Annual review of policies, procedures, and governance structures.

5.7 Enforcement and Sanctions

Non-compliance with this policy may result in disciplinary action, including but not limited to:

- Written warnings.
- Suspension of system access.
- Termination of employment or contractual relationships.
- Reporting to regulatory authorities as required by law.

5.8 Continuous Improvement

- The organization commits to continuous improvement in data protection governance through:
  - Regular training and awareness programs.
  - Benchmarking against best practices.
  - Incorporating lessons learned from audits and incidents.

Chapter Six

6.0 STAFF GUIDE TO DATA PRIVACY

6.1 Purpose

- To inform staff about the organization's data privacy policies and practices.
- To ensure compliance with data protection laws (e.g., NDPA 2023 in Nigeria).
- To guide staff in responsibly handling personal and sensitive data of customers, employees, and third parties.

6.2 Scope

- Applies to all employees, contractors, interns, and third-party service providers with access to personal data.
- Covers all forms of data: electronic, paper, or verbal communications.

6.3 Key Principles

All staff must adhere to core data protection principles:

1. **Lawfulness, Fairness, Transparency:** Process personal data legally and openly.
2. **Purpose Limitation**: Collect data only for specified, legitimate purposes.
3. **Data Minimization**: Only collect data necessary for the intended purpose.
4. **Accuracy:** Keep data up-to-date and accurate.
5. **Storage Limitation:** Retain data only as long as necessary.
6. **Integrity & Confidentiality**: Protect data against unauthorized access, loss, or damage.
7. **Accountability:** Staff must demonstrate compliance with data privacy policies.

6.4 Staff Responsibilities

- Understand and comply with the organization's data protection policies.
- Only access data required for job responsibilities.
- Maintain confidentiality of personal and sensitive information.
- Report data breaches or suspicious activities immediately.
- Attend periodic data protection training.

6.5 Operational Responsibilities

Staff handling data in operational roles must:

1. **Data Collection & Entry**: Ensure accurate, complete, and timely input of data.
2. **Verification:** Confirm the authenticity of documents and information provided by customers or staff.
3. **Data Storage & Security**: Safeguard records using secure systems and follow password, encryption, and physical storage protocols.
4. **Internal Sharing:** Share data only with authorized personnel for operational purposes.
5. **Monitoring & Auditing**: Regularly review operational processes to identify data protection risks.
6. **Incident Response**: Escalate any operational issues affecting data privacy immediately to the Data Protection Officer (DPO).
7. **Backup & Recovery**: Ensure data backups are performed regularly and can be restored in case of loss.

6.6 Data Handling Guidelines

- **Collection:** Obtain consent where necessary. Collect only relevant data.
- **Storage:** Secure data with passwords, encryption, or locked physical storage.
- **Access:** Limit access to authorized personnel only.
- **Sharing:** Share data internally or externally only for legitimate purposes and with proper authorization.
- **Disposal:** Safely destroy or anonymized data that is no longer required.

6.7 Data Breach Reporting

- All staff must immediately report suspected or actual data breaches to the Data Protection Officer (DPO).
- A quick response helps mitigate risk and fulfill regulatory obligations.

6.8 Employee Rights

- Employees have the right to access their personal data held by the organization.
- They can request correction, deletion, or restriction of their personal data as permitted by law.

6.9 Compliance and Sanctions

- Non-compliance with data privacy policies may result in disciplinary action, including warnings, suspension, or termination.

- Staffs are encouraged to seek guidance if uncertain about any aspect of data handling.

6.10 Training and Awareness

- Staff will receive regular training on data privacy obligations and best practices.
- Continuous awareness campaigns will reinforce the importance of data protection.

6.11 Enforcement and Sanctions

Non-compliance may lead to:

- Written warnings
- Suspension of system access
- Termination of employment or contracts
- Regulatory reporting

Summary Statement:

All staffs are custodians of personal and sensitive data. Compliance with this policy manual including operational responsibilities ensures the organization operates legally, ethically, and securely in handling data, protecting both individuals and the company.

APPROVAL

This Data Privacy and Protection Policy is approved by the Board of Directors of Uforo Microfinance Bank Ltd and takes effect from the date of approval.

Approved By: Board of Directors
Effective Date: 1st April, 2025

CHAIRMAN, BOARD OF DIRECTORS **DIRECTOR**