Polyunwana Microfinance Bank

Data Privacy Policy

Table of Contents

1.0 Introduction

As part of our operations, Polyunwana Microfinance Bank Nigeria Limited ("PMFB" or "the Bank") collects and processes the personal information of individuals, organizations or companies which could make such individuals/organization/company easily identifiable. These individuals/organization/company include past, current, and prospective employees, vendors, customers/clients and their representatives, next-of-kins and other individuals the Bank communicates or deals with, jointly and/or severally ("Data Subjects").

Maintaining the Data Subject's trust and confidence requires that Data Subjects do not suffer consequences/effects as a result of providing the Bank with their Personal/organizational/company's Data. To this end, the Bank is firmly committed to complying with applicable data protection laws, regulations, rules, and principles to ensure security of Personal/organization/company Data handled by the Bank. This Data Protection Policy ("Policy") describes the minimum standards that must be strictly adhered to regarding the collection, storage, use and disclosure of Personal/organization/company Data and demonstrates the Bank's dedication and commitment to processing Personal/organizations/company Data it receives or handles with absolute confidentiality and security.

This Policy applies to all forms of systems, operations and processes within the Bank involving the collection, storage, use, transmission, and disposal of personal data.

Failure to comply with the data protection rules and guiding principles set out in the Nigeria Data Protection Act, 2023(NDPR) in addition to those set out in this Policy shall be considered a material violation of the Bank's policies and may result in disciplinary action ..The Nigeria Data Protection Regulation (NDPR) is a piece of legislation that governs how the Bank collects and processes personal/organization/company data. Failure to comply with the NDPR may have severe consequences for the Bank, including potential fines up to 2% of the Bank's annual gross revenue from a preceding year or payment of the sum of N10,000,000 (ten million naira) whichever is greater, for the Bank.

2.0. Scope

This Policy applies to all employees of the Bank, external business partners (such as suppliers, contractors, vendors and other service providers) who receive, send, collect, access, or process Personal Data on behalf of the Bank, including processing that is wholly or partly by automated means. The Policy also applies to third party data processors, who process personal data received from the Bank.

3.0 Objective

The purpose of this Policy is outlined as follows:

- To protect the Bank from the risks of a data breach.
- To disclose how the Bank stores and processes personal data.
- To protect the rights of staff, members, and stakeholders of the Bank.
- To comply with the NDPR, other applicable regulations and follow international best practices as relating to data protection.
- To provide guidelines for ensuring that Customers/Clients data are adequately protected and the highest level of confidentiality maintained.

4.0 Roles and Responsibilities

In compliance with the Regulation, below are some stakeholders and their responsibilities to drive the operationalization of the Policy and implementation of necessary data protection controls within the company.

Board

- Set the tone at the top on data protection
- Ultimately responsible for ensuring that the Bank meets the obligations of the Regulation
- Approve this policy and any subsequent reviews.

Board Finance, Information Technology and General-Purpose Committee

- Approve in conjunction with legal any data protection statements attached to communications such as emails and letters
- Approve in conjunction with legal, responses to any data protection queries from journalist or media outlets such as newspaper
- Review and approve any contracts or agreements with third parties that may handle the Bank's sensitive data

Management Committee

- Ensure data protection objectives are established and are aligned with the strategic direction of the Bank.
- Ensure that the resources needed for the protection of data are available

- Communicate the importance of effective data protection in the Bank and of conforming to its requirements
- Support other relevant Management roles to demonstrate their leadership as it applies to their areas of responsibility
- Provide directives that ensures marketing initiatives abide by data protection principles.

Data Protection Officer

- Keep Management updated about data protection responsibilities, risks, and issues
- Review all data protection procedures and related policies, in line with an agreed schedule
- Arrange data protection training and advice for the people covered by the Policy
- Handle data protection questions from staff and anyone else covered by the Policy

Head, Information Technology

- Ensure all systems, services and equipment used for storing data meet acceptable security standards
- Evaluate any third-party services the Bank is considering using to store or process data such as private cloud computing services
- Perform regular checks and vulnerability scans to ensure adequate security of hardware and software used in data processing.

Head, Internal Audit Department

- Provide reasonable assurance regarding the achievement of the operational objectives, such as the effectiveness and efficiency of the security controls
- Carry out internal audit and report findings to Management/Board
- Recommend preventive and corrective action

5.0 Nigeria Data Protection Regulation

The Regulation, which came into force on January 25, 2019, regulates the gathering, storing and processing of personal data (regardless of whether data is stored electronically, on paper, or on other materials), and protects the rights and privacy of all living individuals (including children). The Regulation applies to natural persons residing in Nigeria or residing outside Nigeria but of Nigeria descent.

6.0 Applicability

Based on the provisions of the NDPR, the Bank will be described as a data controller under the terms of the Regulation – this means the Bank is ultimately responsible for controlling the use and processing of personal/organization/company data. To ensure compliance, the Bank shall appoint a Data Protection Officer

(DPO) for the purpose of ensuring adherence to the NDPR, relevant data privacy statements and data protection directives of the Bank. The contact details of the Data Protection officer are as follows –

The Data Protection Officer
Polyunwana Microfinance Bank
Akanu Ibiam Federal Polytechnic,
Unwana, Ebonyi State.
dataprotectionofficer@polyunwanamfb.com

7.0 General Principles for Processing of Personal Data

The Bank is committed to maintaining the principles in the NDPR regarding the processing of Data. The following basic principles relating to the processing of data are adhered to demonstrate the commitment as well as the Bank's aim of creating a positive privacy culture:

7.1 Lawfulness, Fairness and Transparency

Data must be processed lawfully, fairly and transparently at all times, as such, data collected and processed by or on behalf of the Bank must be pursuant to a specific, legitimate and lawful purpose consented to by the Data Subject, save where the processing is otherwise allowed by law or within other legal grounds recognized in the NDPR.

7.2 Data Accuracy

Data must be accurate and kept up to date. In this regard, the Bank shall make reasonable efforts to ensure the following:

a) Data collected and/or processed are accurate and not misleading in a manner that could be harmful to the Data Subject.
b) Reasonable and Applicable data are regularly updated
c) Timely correction of data on discovery of inaccuracies.

7.3 Purpose Limitation

The Bank collects personal data for the purposes identified in the Bank's privacy notice or other relevant document, based on any non–written communication (where applicable), provided to the Data Subject and for which consent is collected. Such data shall not be reused for purposes incompatible with those originally agreed, unless further consent is obtained.

7.4 Data Minimization

- The Bank limits data collection and usage to data that is relevant, adequate, and necessary for carrying out the purpose for which such data is processed.
- The Bank will evaluate the extent and need for processing data and where allowed, anonymized data must be used.

7.5 Integrity and Confidentiality

- The Bank shall establish adequate controls to protect the integrity and confidentiality of data, both in digital and physical format and to prevent data from being accidentally or deliberately compromised.
- Data of Data Subjects must be protected from unauthorized access or viewing and from unauthorized changes to ensure its correctness.
- Any processing of data by an employee without a mandate to perform such will be considered unauthorized and shall attract internal disciplinary actions.
- Employees may access personal data only as is appropriate for the type and scope of task in question and are forbidden to use such data for their own private or commercial purposes or to disclose or make such available to unauthorized persons.
- The Human Resources Department must inform employees at the start of the employment relationship of the obligation to maintain data privacy. This obligation shall remain in force even after an employees' employment ceases.

7.6 Accountability

- The Bank shall show accountability consistent with the NDPR obligations by monitoring and continuously improving data privacy practices within the Bank.
- Any individual or employee in breach of this Policy shall be subject to internal disciplinary action and could also face civil or criminal liability where their actions violate the law.

8.0 Data Privacy Policy

8.1 Overview

The Bank considers customers data as confidential, and strives to adequately protect such data from unauthorized use and/or disclosure. The Bank shall ensure that the Data Subjects are provided with adequate information regarding the use of their data as well as secure their requisite consent, where necessary. Also, the Bank shall display a simple, visible and clear notice (Privacy policy) on any medium through which customers data is being collected or processed. The following information shall be considered for inclusion in the Privacy policy, as appropriate in distinct circumstances in order to ensure fair and transparent processing:

a) Data subjects' consent.
b) Description of collectable information.
c) Purpose of collection of data.
d) Technical methods used to collect and store information, cookies, web tokens, etc.
e) Access, if any, of third parties to data and purposes of such access.

f) A highlight of the principles governing data processing.

g) Available remedies in event of a violation of the privacy policy.

h) The timeframe for remedy.

i) Any limitation clause, provided that such limitation clause does not exonerate the operator from breaches of the Regulation

Pursuant to its statutory mandate of rendering Microfinance Banking Services in which the Bank received license from Central Bank of Nigeria to do, **Polyunwana Microfinance Bank Nigeria Limited** (the Bank) collects and takes custody of data of customers (personal, organization, company) and their related persons, such as beneficiaries and next-of-kins and their employers. The data include, but are not limited to, the biodata of customers and related persons.

This Data Privacy Policy (the Policy) is, therefore, instituted by the Bank to inform customers and other related persons of the protection of their data collected and stored by the bank's pursuant to the performance of its business and service responsibilities. The Policy also explains how the data are collected, stored and used. It highlights the few exceptional instances for disclosed.

8.1.1 Nature and reason for collection of personal data

In order to provide adequate and satisfactory banking services and in line with extant regulations, the Bank collects data of customers and their related persons. These may include name, gender, marital status, date of birth, nationality, National Identification Number, employment information and Next-of-Kin Information, business name, address, Corporate Affairs Commission registration documents, Personal Details of Directors amongst others.

Data collected and processed by the Bank may include but are not limited to:

a) Contact data (e.g. name, telephone, e-mail, address, IP address).

b) Customer's account details

c) Information about next of kin

d) Disclosed information (from third parties).

e) Employee and prospective employee data collected for recruitment and onboarding purpose.

Methods adopted by the Bank in the collection and storage of data may include but are not limited to:

a) Cookies.

b) CCTV recordings.

c) Physical and Online Forms

d) External hard drive

e) Audio and video call recordings

The Bank collects the data of a customer or prospective customer and to render Banking services to the customer. In this regard, it is necessary, to collect some private data of customers to ensure that uniquely identifiable client are registered in the Bank's Database. It also facilitates the accurate classification of customers and proper service rendition processes.

8.2 Consent of Data Subject

Collection of customers data by the Bank shall be subject to the consent and authorization of the Data Subjects. Consequently, account opening, loan application, loan renewal, overdraft, employee, atm request, ussd request, fixed deposit, fund transfer and client update forms, including the electronic formats, contain data authorization clauses which are activated when the data subject completes the form.

8.3.1 Procuring Consent

Where the processing of customers Data is based on consent, the Bank shall obtain the requisite consent of the data subjects at the time of collection of customer Data. In this regard, the Bank will ensure:

a) that Customer Data is not obtained except the specific purpose of collection is made known to the data subject

b) that the consent of Data Subject has been obtained without fraud, coercion, or undue influence

c) that the data subject has consented to processing of his or her data and has the legal capacity to give consent, where processing is based on consent

d) that request for consent is in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language, where the data subject's consent is given in the context of a written declaration

e) that the Data Subject is informed of his/her right

f) that when assessing whether consent is freely given, the Bank shall take account of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of customer data that is either not necessary or excessive for the performance of the contract

g) that the consent of the data subject is obtained where data may be transferred to a third party for any reason.

8.3.2 Valid Consent

For consent to be valid, it must be given voluntarily by an appropriately informed Data Subject. In line with regulatory requirements, Consent cannot be implied. Silence, or inactivity does not constitute Consent under the NDPR.

8.3.3 Consent of Minors

The consent of minors (under the age of 18) will always be protected and obtained from minor's representatives following applicable regulatory requirements

8.4 Processing and Protection of Personal Data

The Bank shall process the data of customers and other related persons only for the purpose for which the data is collected. The Bank shall process such data on both electronic and manual platforms, as may be required.

Only authorized officers of the Bank shall have access to the data of Customers and related persons collected. In line with the Bank policies, such authorized persons shall include every member of the Board, employee, agent or any other person engaged or authorized by the Bank to examine any document or make an inquiry in relation thereto. Such authorized persons have a confidentiality obligation not to disclose or use any information or data of such person/entity obtained directly or indirectly, except under the express authority of the Bank or as otherwise provided for under this Policy.

8.5 Storage and Retention of Personal Data

7.5.1: The Bank shall securely store the data of customers and related persons that it collects in hard paper copies, computers, servers, and other electronic devices.

7.5.2: The Bank shall hold Data of customers and related persons for as long as may be deemed necessary to keep track of customers activities in the Bank. The retention period shall however not be less than 10 years, in line with the provisions of the National Archives Act, CAP.N6 Laws of the Federation of Nigeria, 2004.

8.6.0 Disclosure of Personal Data

8.6.1: Without prejudice to the foregoing provisions, however, the Bank may be obliged to disclose personal data in its custody in the following circumstances:

- Where disclosure is made in compliance with statutory obligation or under an order of a court of competent jurisdiction.

- Where the Data Owner has expressly consented to the disclosure or instructed that his/her data be fully or partially disclosed to a named person or organization; Provided that such consent or instruction may be withdrawn and communicated to the Bank in writing at any time before disclosure.

Where the disclosure is made to the named person or organization for his/her use or record.

8.6.2 Transfer of Personal Data

Customer's data can only be transferred to Third Party Data Processing Contracts. To ensure compliance with the Regulation, being a Data Controller, the Bank shall:

- Ensure that a written contract is signed by a third party that will process personal data of individuals/organizations.

- Ensure that such third party that will process the data obtained from data subjects, complies with applicable laws and regulations

8.6.3 Transfer of Personal Data to Foreign Country

Where Customer Data is to be transferred to a country outside Nigeria, the Bank shall put adequate measures in place to ensure the security of such Customer Data. In particular, the Bank shall, among other things, conduct a detailed assessment of whether the said country is on the National Information Technology Development Agency (NITDA) White List of Countries with adequate data protection laws.

The Bank shall comply with the Regulation and any transfer of customer data that is undergoing processing or is intended for processing after transfer to a foreign country or an international organization, shall take place subject to the provisions of the Regulation.

8.6.4 Exceptions in Respect of Transfer to a Foreign Country

In the absence of any decision made by NITDA or the Honorable Attorney General of the Federation (HAGF) on the transfer of customer data to a foreign country, the operator shall initiate the transfer or set of transfers of customer data to such foreign country or an international organization only when:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers to the data subject due to the absence of an adequate decision and appropriate safeguards and that there are no alternatives.
- The transfer is necessary for the performance of a contract between the data subject and the Bank or the implementation of pre-contractual measures taken at the data subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the operator and another natural or legal person
- The transfer is necessary for important reasons of public interest

- The transfer is necessary for the establishment, exercise, or defense of legal claims
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

The Bank, in compliance with the Regulation, shall explicitly communicate through clear warnings, the specific principle(s) of data protection that is likely to be violated in the event of a transfer to a third country.

9.0 Violation of Data Privacy and Remedies

Employees, customers or their related persons whose data privacy rights are violated under this Policy shall report in writing, such violation to the Bank for immediate redress. The Bank shall immediately restore the rights of the customer, employee or related person failing which the affected person/entity may take legal actions seeking for redress in line with Nigerian Data Protection Regulation, 2019.

10.0 Governing Laws

This Data Privacy Policy is consistent with Sections 13 of the Constitution of the Federal Republic of Nigeria 1999 (as amended). It is also consistent with Clause 2.5 (a-i) of the Nigeria Data Protection Regulation 2019 issued by the National Information and Technology Development Agency (NITDA) and Article 8 of the International Convention on Data Protections.

11.0 Rights of Data Subjects

The Bank shall:

- Take appropriate measures to provide any information relating to processing, to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child
- Provide such information in writing, or by other means, including, where appropriate, by electronic means
- Provide any information relating to the processing of data obtained from the data subject orally, at the request of the data subject, provided that the identity of the data subject is proven by other means
- Inform the data subject without delay and at least within one (1) month of receipt of a request relating to the processing of his/her data, the reasons for not providing the information and the possibility of lodging a complaint with the supervisory authority
- Provide information, any form of communication or any actions taken to a data subject free of charge

- Charge data subject if the request for his/her data is manifestly unfounded or excessive, in particular because of his/her repetitive character. The charge shall be a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested
- Write a letter to the data subject stating "refusal act" on the request and copy NITDA on every occasion through a dedicated channel which shall be provided for such purpose, provided that such request is excessive
- Bear the burden of demonstrating the manifestly unfounded or excessive character of the request
- Request for provision of additional information necessary to confirm the identity of the data subject where the operator has reasonable doubts concerning the identity of the requestor

- Provide the information in combination with standardized icons in order to give in an easily visible, intelligible, and legible manner, a meaningful overview of the intended processing and machine-readable format when presented electronically
- Provide the data subject with all of the following information, before collecting personal data:
    - The contact details of the Data Protection Officer
    - The purposes of the processing for which the customer data are intended as well as the legal basis for the processing
    - The legitimate interests pursued by the operator or by a third party
    - The recipients or categories of recipients of the customer data, if any
    - The period for which the customer data will be stored, or if that is not possible, the criteria used to determine that period
    - The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
    - The right to lodge a complaint with a relevant authority
    - Whether the provision of customer data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the customer data and of the possible consequences of failure to provide such data
    - The existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- Inform the data subject of the appropriate safeguards for data protection in the foreign country
- Rectify, without undue delay, inaccurate customer data concerning data subjects per their request

- Acknowledge the right of data subjects to have their incomplete data completed, including utilizing supplementary statement
- Delete customer data where one of the following grounds applies:
    - The customer data are no longer necessary in relation to the purposes for which they were collected or processed
    - The data subject withdraws the consent on which the processing is based
    - The data subject objects to the processing and there are no overriding legitimate grounds for the processing
    - The customer data have been unlawfully processed
    - The customer data have to be erased for compliance with a legal obligation in Nigeria
- Take all reasonable steps to delete all the customer data made public and inform other companies/Banks processing the customer data of the data subject's request
- Acknowledge data subjects' rights to obtain restriction of processing their data where one of the following applies:
    - The accuracy of the data is contested by the data subject for a period enabling the operator to verify the accuracy of the data
    - The processing is unlawful, and the data subject opposes the erasure of the data and requests the restriction of their use instead
    - The Bank no longer needs the data for processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims
    - The data subject has objected to processing pending the verification to confirm whether the legitimate grounds of the operator override those of the data subject
- Process data with the data subject's consent, where processing has been restricted
- Communicate any rectification or erasure of data or restriction to each recipient to whom the data has been disclosed, unless this proves impossible or involves disproportionate effort
- Provide data concerning data subjects, in a structured manner, commonly used and machine-readable format to such data subjects
- Not hinder the data subject from transmitting those data in its database to another Bank/company where the processing is based on consent, on a contract and processing is carried out by automated means
- Execute data subjects' requests on the transmission of their data to another company/Bank, where technically feasible.at a reasonable cost.

Data Subjects can exercise any of their rights by writing to the Bank of their intents via dataprotectionofficer@polyunwanamfb.com

12.0 Data Breach Management Procedure

A data breach procedure is established and maintained in order to deal with incidents concerning Data or privacy practices leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data transmitted, stored or otherwise processed.

All employees must inform their respective Head of Department or the Data Processing Officer of the Bank immediately about cases of violations of this Policy or other regulations on the protection of Customer Data, following the Bank's Customer Data Breach Management Procedure in respect of any:

a) improper transmission of Customer Data across borders.
b) loss or theft of data or equipment on which data is stored.
c) accidental sharing of data with someone who does not have a right to know this information.
d) inappropriate access controls allowing unauthorized use.
e) equipment failure.
f) human error resulting in data being shared with someone who does not have a right to know; and
g) hacking attacks.

12.1 Notification

A data protection breach notification must be made immediately after any data breach occurs. This is to ensure that the supervisory authority shall at least:

- describe the nature of the data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned.
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.
- describe the likely consequences of the data breach.
- describe the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects.

In case there is a significant chance of adverse effects on the data subject, the data subject is also duly notified about the breach. The information given includes that:

a) the controller has implemented appropriate technical and organizational protection measures and those measures were applied to the data affected by the data breach, in particular those that render the data unintelligible to any person who is not authorized to access it.

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

12.2 Potential Breach

When a potential breach has occurred, the Bank will investigate to determine if an actual breach has occurred and the actions required to manage and investigate the breach as follows:

a) Validate the Customer Data breach.

b) Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded.

c) Identify remediation requirements and track resolution.

d) Report findings to the top management.

e) Coordinate with appropriate authorities as needed.

f) Coordinate internal and external communications; and

g) Ensure that impacted Data Subjects are properly notified, if necessary.

Reporting of data breach to a Data Protection Authority is very important under the NDPR. Data breaches are to be reported within 72 hours after becoming aware of it

.13.0 Data Protection Impact Assessment

As part of the risk and audit assessment, the Bank shall carry out a Data Protection Impact Assessment (DPIA) in respect of any new project or IT system involving the processing of Customer Data to determine whenever a type of processing is likely to result in any risk to the rights and liberties of the Data Subject.

14.0 Data Security

All Customers Data must be kept securely and should not be stored any longer than necessary. The Bank will ensure that appropriate measures are employed against unauthorized access, accidental loss, damage, and destruction to data. This includes the use of password, encryption of databases for digital storage and locked cabinets for those using a paper form.

To ensure the security of Customer Data, the Bank will, among other things, implement the following appropriate technical controls:

a) Develop security measures including but not limited to protecting systems from hackers

b) Set up firewalls and protect email systems

c) Store data securely with limited access to specifically authorized individuals

d) Employ data encryption technologies on workstation/laptops. Also implementing encryption at rest including key management

e) Develop an organizational policy for handling customer data and other sensitive or confidential data

f) Continuously build capacity for all staff

g) Industry-accepted hardening standards i.e. enhancing the system's security features which include (the use of strong passwords for authentication, minimizing unnecessary software etc.), for workstations, servers, and databases.

h) Restrict the use of removable media such as USB flash, disk drives.

i) Anonymization techniques on testing environments; and

j) Physical access control where Customer Data is stored in hardcopy.

15.0 Personnel Training

The Bank shall ensure that employees who collect, access and process Customers Data receive adequate data privacy and protection training in order to develop the necessary knowledge, skills and competence required to effectively manage the compliance framework under this Policy and the NDPR concerning the protection of Customer's Data. On an annual basis, the Bank shall develop a capacity building plan for its employees on data privacy and protection in line with the NDPR.

16.0 Data Protection Audit Assessment

The Bank shall conduct periodic data protection audits through a licensed Data Protection Compliance Organization (DPCOs) to verify the company's compliance with the provisions of the NDPR and other applicable data protection laws.

The audit report will be certified and filed by the DPCO to NITDA as required under the NDPR.

17.0 Definitions

- **"NDPR"** means the Nigerian Data Protection Regulation, 2019.

- **"Customer Data"** means any information relating to an identified person or entity ('Data Subject'); an identifiable person or entity is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural entity; It can be anything from a name, address, a photo, an email address, bank details, PIN

number, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.

- **"Sensitive Personal Data"** means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records, or any other sensitive personal information.
- **"Consent"** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
- **"Data"** means characters, symbols and binary, on which operations are performed by a computer which may be stored or transmitted in the form of electronic signals stored in any format or any device
- **"Database"** means a collection of data organized in a manner that allows access, retrieval, deletion and procession of that data; it includes but not limited to structured, unstructured, cached and file system type databases
- **"Data Administrator"** means a persons or organization that processes data
- **"Data Controller"** means a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and how personal data is processed or is to be processed
- **"Data Portability"** means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format
- **"Nigeria Information Technology Development Agency"** - NITDA
- **"Data Protection Compliance Organization"** (DPCO) means any entity duly licensed by NITDA for training, auditing, consulting and rendering services and products for compliance with this Regulation or any foreign Data Protection law or regulation having effect in Nigeria
- **"Data Subject"** means an identifiable person; one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity
- **"Party"** means directors, shareholders, servants, and privies of a contracting party
- **"Processing"** means any operation or set of operations which is performed on customer data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- **"Personal Data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed
- **"Record"** means public record and reports in a credible news media
- **"Regulation"** A rule or instruction made and maintained by an authority

18.0 Review and Enquiries

This Privacy Policy is subject to review by the Bank from time to time as the need arises. All enquiries regarding the Policy should be directed to:

The Managing Director,

Polyunwana Microfinance Bank,

Akanu Ibiam Federal Polytechnic,
Unwana

19.0 Consequences

The consequence of not adhering to the Policy will be handled in line with the Bank's Relevant Policy.

For: Polyunwana Microfinance Bank

Nkeiruka Nkem Oko
Managing Director

Engn.Tech Chibueze Ogbulafor
Head Information Technology
/Data Protection Officer