1. Introduction

is committed to conducting its business in accordance with all applicable Data Protection laws and Policies and in line with the highest standards of ethical conduct.

This policy details expected behaviours of xxxx’s Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a ’s Customers and Staff (i.e. the Data Subject) and irrespective of the media used to store the information.

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other Policys, which impose restrictions on how organisations may process Personal Data.

An organisation that handles personal data and makes decisions about its use is known as a Data Controller. , as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy.

Non-compliance may expose to complaints, regulatory action, fines and/or reputational damage.

’s leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Employees and Third Parties to share in this commitment.

1. Scope
   1. This policy applies to all Entities where a Data Subject’s personal data is processed:
      * in the context of the business activities of the Entity
      * for the provision or offer of ing services to individuals by
      * to actively monitor the behaviour of individuals.
      * in relation to natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent.
      * with the intention of not denying any Nigerian or natural person the privacy rights, he is entitled to under any law, Policy, policy, contract, for the time being in Nigeria or in any foreign jurisdiction.
   2. Monitoring the behaviour of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:
      * taking a decision about them
      * analysing or predicting their personal preferences, behaviours and attitudes.
   3. This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.
   4. The Data Protection Officers (DPOs) are responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. The DPOs within are:
   5. Please contact the DPO with any questions about the operation of this Privacy Standard or the Nigeria Data Protection Policy or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:
      * if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company)
      * if you need to rely on Consent and/or need to capture Explicit Consent
      * if you need to draft Privacy Notices or Fair Processing Notices
      * if you are unsure about the retention period for the Personal Data being Processed
      * if you are unsure about what security or other measures you need to implement to protect Personal Data
      * if there has been a Personal Data Breach
      * if you are unsure on what basis to transfer Personal Data outside Nigeria
      * if you need any assistance dealing with any rights invoked by a Data Subject
      * if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making
      * if you need help complying with applicable law when carrying out direct marketing activities; or
      * if you need help with any contracts or other areas in relation to sharing Personal Data with Third Parties (including our vendors).
2. **Definitions**

In this Policy document, unless the context otherwise requires:

1. “Act” means the National Information Technology Development Agency Act of 2007;
2. “Computer” means Information Technology systems and devices, whether networked or not;
3. ‘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;
4. 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 is stored in any format or any device;
5. “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;
6. “Data Administrator “means a person or organization that processes data
7. “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;
8. “Database Management System” means software that allows a computer to create a database, add, change or delete data in the database; allows data in the database to be processed, sorted or retrieved;
9. “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;
10. Data Protection Compliance Organisation (DPCO) means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this Policy or any foreign Data Protection law or Policy affecting Nigeria;
11. “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;
12. “Data Subject Access Request” means the mechanism for an individual to request a copy of their data under a formal process and payment of a fee;
13. “filing system” means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
14. “Foreign Country” means other sovereign states, autonomous or semi-autonomous territories within the international community;
15. NDPR –Nigeria Data Protection Regulation
16. “Policy” means this Policy and its subsequent amendments and where circumstance requires it shall also mean any other Policy on the processing of information relating to identifiable individual’s Personal Data, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use, or disclosure
17. Personal Data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person 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 person; It can be anything from a name, address, a photo, an email address, details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others;
18. Processing” means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
19. Personal Data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
20. “Recipient” means a natural or legal person, a public authority who accepts data;
21. “Relevant Authorities” means the National Information Technology Development Agency (NITDA) or any other statutory body or establishment having a government mandate to deal solely or partly with matters relating to personal data;
22. “Sensitive Personal Data” means Data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information;
23. The Agency” means the National Information Technology Development Agency and
24. “Third Party” means any natural or legal person, public authority, establishment or any other body other than the Data Subject, the Data Controller, the Data Administrator and the persons who are engaged by the Data Controller or the Data Administrator to process personal data.

4 Policy

### Governance

* + 1. Policy Dissemination and Enforcement

The management team of must ensure that all Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy. Also, will make sure all Third Parties engaged to Process and use Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, before granting them access to Personal Data controlled by .

* + 1. Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

* + 1. Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by , will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess compliance with this policy and the operational practices about the protection of Personal Data, including:

* the personally identifiable information the organization collects on employees of the organization and members of the public;
* any purpose for which the personally identifiable information is collected;
* any notice given to individuals regarding the collection and use of personal information relating to that individual;
* any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
* whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent;
* the policies and practices of the organization for the security of personally identifiable information;
* the policies and practices of the organization for the proper use of personally identifiable information;
* organization policies and procedures for privacy and data protection;
* the policies and procedures of the organization for monitoring and reporting violations of privacy and data protection policies; and
* the policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.

Any major deficiencies identified will be reported to and monitored by Executive Management team.

**Principles**

* + 1. Data Protection

### has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data.

|  |  |
| --- | --- |
| **PRINCIPLE** | **DEFINITION** |
| Principle 1: Lawfulness, Fairness and Transparency | Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness). |
| Principle 2: Purpose Limitation | Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.  Further processing may be done only for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.  Any person or entity carrying out or purporting to carry out data processing under the provision of the above paragraph shall not transfer any personal data to any person. |
| Principle 3: Data  Minimisation | Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed. This means must not store any Personal Data beyond what is strictly required. |
| Principle 4: Accuracy | Personal Data shall be accurate and kept up to date. This means must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data. |
| Principle 5: Storage Limitation | Personal Data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject. |
| **Principle 6:** Integrity & Confidentiality | Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, all foreseeable hazards and breaches such as theft, cyber-attack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements and against accidental loss, destruction or damage. must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data are maintained at all times.  Anyone who is entrusted with the personal data of a data subject or who is in possession of the personal data of a data subject owes a duty of care to the said data subject; |

### Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance. This means must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

### Data Collection

* No data shall be obtained except the specific purpose of collection is made known to the Data Subject.
* Data Controller is under obligation to ensure that consent of a Data Subject has been obtained without fraud, coercion or undue influence.

# Third party data processing contracts

Data processing by a third party shall be governed by a written contract between the third party and the Data Controller. Accordingly, any person engaging a third party to process the data obtained from Data Subjects shall ensure adherence to this Policy

# 4.4 Privacy policy

Notwithstanding anything contrary in this Policy or any instrument for the time being in force, any medium through which personal data is being collected or processed shall display a simple and conspicuous privacy policy that the class of Data Subjects being targeted can understand. The privacy policy shall, in addition to any other relevant information, contain the following:

1. what constitutes the Data Subject’s consent;
2. description of collectable personal information;
3. purpose of collection of personal data;
4. technical methods used to collect and store personal information
5. access (if any) of third parties to personal data and purpose of access;
6. a highlight of the principles stated.
7. available remedies in the event of a violation of the privacy policy;
8. the time frame for remedy and
9. any limitation clause provided that no limitation clause shall avail any Data Controller who acts in breach of the principles of lawfulness.

4.5 Objections by the data subject

The right of a Data Subject to object to the processing of his data shall always be safeguarded. Accordingly, a Data Subject shall have the option to:

1. object to the processing of personal data relating to him which the Data Controller intends to process for the purposes of marketing;
2. be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge.

# 4.6 Transfer to a foreign country

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a foreign country or an international organisation shall take place subject to the other provisions of this Policy

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## 

## Document Ownership

This Policy is owned by the YYYY.

## Document Coordinator

This Policy is coordinated by the YYYY.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## 

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff