DATA PROTECTION POLICY

The Chartered Institute of Bankers of Nigeria

Last updated	January 2021

Definitions

Institute	means The Chartered Institute of Bankers of Nigeria
NITDA	means the National Information Technology Development Agency
The Regulation	means the Nigeria Data Protection Regulation 2019.
Computer"	means Information Technology systems and devices, networked or not;
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, through a statement or 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;
Databas	means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type databases;
Database Management System	means a 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;
Data Subject	means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
Processing	means any operation or set of operations which is performed on Personal Data or on 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;

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, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to Media Access Control (MAC) address, Internet Protocol (IP) address, International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, subscriber identification module (SIM), Personal Identifiable Information (PII) and others;
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;
Data Controller	Is the Chartered Institute of Bankers of Nigeria.
Data Administrator	Is the Head, Information Communications Technology
Data Protection Officer	Is the Head, Internal Audit and Compliance
Register of Systems	means a register of all systems or contexts in which personal data is processed by The Chartered Institute of Bankers of Nigeria.

1.0 Data protection principles

The Institute is committed to processing data in accordance with its responsibilities under the Regulation.

1.1 personal data shall be:

a. collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject; provided that:

   i. a further processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest;

   ii. any person or entity carrying out or purporting to carry out data processing under the provision of this paragraph shall not transfer any Personal Data to any person;

b. adequate, accurate and without prejudice to the dignity of human person;

c. stored only for the period within which it is reasonably needed, and

d. secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.

1.2 Duty of Care

a. Person entrusted with 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 Data Subject;

b. Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject shall be accountable for his acts and omissions in respect of data processing, and in accordance with the principles contained in this Regulation.

2.0 General provisions

a. This policy applies to all personal data processed by the Institute.
b. This policy shall be reviewed at least annually.

3.0 Lawful Processing

Without prejudice to the principles set out in this Policy, the Institute shall:

a. Obtain the consent of the Data Subject to process his or her personal data for one or more specific purposes;
b. Ensure that the processing is necessary for compliance with a legal obligation to which the Controller is subject
c. Ensure that the processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
d. Ensure that individuals are afforded the right to access their personal data and any such requests made to the Institute shall be dealt with in a timely manner.

4.0 Lawful purposes

All data processed must be done on one of the following lawful bases

4.1 Procuring Consent

a. No data shall be obtained except the specific purpose of collection is made known to the Data Subject;

b. Data Controller is under obligation to ensure that consent of a Data Subject has been obtained without fraud, coercion or undue influence; accordingly:

c. if the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is

clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding on the Data Subject;

d. prior to giving consent, the Data Subject shall be informed of his right and method to withdraw his consent at any given time. However, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;

e. when assessing whether consent is freely given, utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of Personal Data that is not necessary (or excessive) for the performance of that contract; and where data may be transferred to a third party for any reason whatsoever

f. where processing is based on consent, the Controller shall be able to demonstrate that the Data Subject has consented to processing of his or her Personal Data and the legal capacity to give consent;

4.2 Due Diligence and Prohibition of Improper Motives

a. No consent shall be sought, given or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts;

b. The Institute shall take reasonable measures to ensure that the other party in any data processing contract does not have a record of violating the principles set out in NITDA or a regulatory authority for data protection within or outside Nigeria;

4.3 Data Security

The Institute shall develop security measures to protect data; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, developing organizational policy for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

4.4 Third Party Data Processing Contract

Data processing by a third party shall be governed by a written contract between the third party and the Institute.

4.4 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:

a) object to the processing of Personal Data relating to him which the Data Controller intend to process for the purpose of marketing;

b) be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge.

4.5 Advancement of Right to Privacy

Notwithstanding anything to the contrary in this Policy, the privacy right of a Data Subject shall be interpreted for the purpose of advancing and never for the purpose of restricting the safeguards Data Subject is entitled to under any data protection instrument made in furtherance of fundamental rights and the Nigerian laws.

5. Data minimisation

a. The Institute shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Institute shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Institute shall consider what data should/must be retained, for how long, and why.

8. Security

a. The Institute shall ensure that personal data is stored securely using modern software, shall employ data encryption technologies and appropriate firewall that are kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. Appropriate back-up and disaster recovery solutions shall be in place.
d. Ensure continuous capacity building of Staff handling personal data.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Institute shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the NITDA (more information on the NITDA website).