Information Management Draft Quality Assurance Policy



|  |  |
| --- | --- |
| **Responsible Executive** | **Vice Chancellor** |
| **Responsible Division** | **Directorate of Quality Assurance** |
| **Approved By** |  |
| **Date Approved** |  |
| **Review Date** | **After every four (4) years** |
| **Stakeholders affected by this policy** | **All categories of staff and students of University of Nigeria Nsukka as well as their partners (JAMB, ALUMINI, FGN and local and International**  **collaborators)** |

Table of Contents

[1. Purpose 2](#_Toc180970361)

[2. Scope 2](#_Toc180970362)

[3. Guiding Principles 2](#_Toc180970363)

[4. Policy Statements 2](#_Toc180970364)

[4.1 Information Collection and Storage 2](#_Toc180970365)

[4.2 Information Access and Usage 2](#_Toc180970366)

[4.3 Data Quality and Integrity 3](#_Toc180970367)

[4.4 Data Security and Protection 3](#_Toc180970368)

[4.5 Records Retention and Disposal 3](#_Toc180970369)

[5. Responsibilities 3](#_Toc180970370)

[6. Monitoring and Evaluation 4](#_Toc180970371)

[7. Policy Review and Revision 4](#_Toc180970372)

# 1. Purpose

This policy establishes standards and guidelines for the management of information across the University of Nigeria. It ensures that all information assets are protected, accessible, accurate, and used responsibly to support the university’s teaching, research, and operational needs.

# 2. Scope

This policy applies to all forms of information within the university, including digital, physical, confidential, and publicly available information. It covers all students, faculty, administrative staff, and third-party contractors who handle, access, or manage university information.

# 3. Guiding Principles

* **Confidentiality and Privacy:** Protect personal, academic, and institutional data to maintain privacy and confidentiality.
* **Integrity and Accuracy:** Ensure that all information is accurate, complete, and maintained with integrity to support reliable decision-making.
* **Accessibility and Availability:** Facilitate timely access to information for authorized users while protecting information assets from unauthorized access.
* **Accountability and Compliance:** Ensure compliance with relevant data protection laws, university policies, and regulatory requirements while promoting accountability among users.

# 4. Policy Statements

## 4.1 Information Collection and Storage

* + Collect and store information based on its relevance to the university’s academic, administrative, and operational activities.
  + Implement standardized procedures for data entry, verification, and validation to ensure accuracy and completeness.
  + Store data securely in a manner that prevents unauthorized access, loss, or damage, with specific protocols for sensitive or confidential information.

## 4.2 Information Access and Usage

* + Ensure that information is accessible only to authorized individuals based on roles, responsibilities, and need-to-know principles.
  + Promote responsible use of information, encouraging users to follow ethical standards and avoid unauthorized sharing, alteration, or misuse.
  + Educate users on information security practices, including strong password policies, secure device usage, and awareness of phishing and other cybersecurity risks.

## 4.3 Data Quality and Integrity

* + Establish processes for regular data audits and updates to maintain data quality, including correcting inaccuracies and eliminating outdated or redundant information.
  + Implement data integrity controls, such as versioning, data validation, and backup protocols, to protect data from corruption and ensure consistency.
  + Encourage a culture of accountability, where users are responsible for maintaining data integrity and reporting discrepancies.

## 4.4 Data Security and Protection

* + Enforce robust cybersecurity measures, including firewalls, encryption, and multi-factor authentication, to protect information systems from unauthorized access and cyber threats.
  + Comply with relevant data protection regulations, such as GDPR or national data protection laws, by implementing appropriate security controls and privacy protocols.
  + Develop incident response procedures to address potential data breaches, including notification, containment, and recovery steps.

## 4.5 Records Retention and Disposal

* + Define retention schedules for various types of information, ensuring compliance with legal, regulatory, and institutional requirements.
  + Implement secure disposal procedures for physical and digital records to prevent unauthorized access or data leakage, using methods such as shredding or digital data wiping.
  + Maintain documentation of retention and disposal practices for accountability and compliance purposes.

# 5. Responsibilities

* **University Leadership** (e.g., CIO, Data Protection Officer) oversees information management practices, ensuring alignment with legal requirements, institutional policies, and best practices.
* **IT and Data Management Teams** are responsible for implementing and maintaining data security, access control, and data integrity measures.
* **Academic and Administrative Departments** follow established guidelines to manage and protect information within their units, ensuring compliance with policy standards.
* **All Staff, Faculty, and Students** are expected to handle information responsibly, adhering to this policy and reporting security or data integrity concerns.

# 6. Monitoring and Evaluation

* **Data Audits:** Conduct regular audits of data management practices to ensure compliance with the policy and identify areas for improvement.
* **User Training and Awareness Programs:** Offer regular training sessions on data privacy, security protocols, and responsible information use for all users.
* **Continuous Improvement:** Use audit findings, user feedback, and incident reports to improve information management processes and update policies as needed.

# 7. Policy Review and Revision

This policy will be reviewed every five years or as necessary to reflect advancements in information management practices, changing regulations, or evolving institutional requirements.