AL MUHIBBAH OPEN UNIVERSITY (AOU), ABUJA**

Data Protection Policy

Ratified by the Senate of AOU, Abuja

July, 2024

Table of Contents

INTRODUCTION

Al Muhibbah Open University (AOU) is committed to protecting the privacy and security of personal data in accordance with Nigeria's Data Protection Act of 2023 and international best practices. This policy outlines our approach to data protection, ensuring the rights of individuals are upheld and data is managed responsibly.

PURPOSE

The purpose of this Data Protection Policy is to:

1. Ensure compliance with Nigeria's Data Protection Act of 2023 and relevant international standards.
2. Protect the rights and privacy of individuals whose data we process.
3. Establish clear guidelines for the collection, use, storage, sharing, and destruction of personal data.
4. Promote transparency and accountability in our data protection practices.

SCOPE

This policy applies to all employees, students, contractors, and third parties who process personal data on behalf of AOU. It covers all personal data, regardless of the medium in which it is held (e.g., electronic, paper).

LEGAL AND REGULATORY FRAMEWORK

AOU's data protection practices are governed by the following regulations and standards:

1. Nigeria Data Protection Act of 2023
2. International best practices, including the General Data Protection Regulation (GDPR) of the European Union where applicable.

DATA PROTECTION PRINCIPLES

AOU adheres to the following data protection principles:

1. Lawfulness, Fairness, and Transparency:
   a. Personal data shall be processed lawfully, fairly, and in a transparent manner.
2. Purpose Limitation:
   a. Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. Data Minimization:
   a. Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. Accuracy:
   a. Personal data shall be accurate and, where necessary, kept up to date.
5. Storage Limitation:
   a. Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.
6. Integrity and Confidentiality:

a. Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

7. Accountability:
   a. AOU shall be responsible for, and be able to demonstrate compliance with, these principles.

DATA SUBJECT RIGHTS

Individuals whose data is processed by AOU have the following rights:

1. Right to Access:
   a. Individuals have the right to access their personal data and obtain information about how it is being processed.
2. Right to Rectification:
   a. Individuals have the right to have inaccurate personal data corrected or completed if it is incomplete.
3. Right to Erasure:
   a. Individuals have the right to request the deletion or removal of their personal data under certain conditions.
4. Right to Restrict Processing:
   a. Individuals have the right to request the restriction or suppression of their personal data under certain conditions.
5. Right to Data Portability:
   a. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
6. Right to Object:
   a. Individuals have the right to object to the processing of their personal data under certain conditions.
7. Rights Related to Automated Decision-Making:
   a. Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

DATA COLLECTION

1. Lawful Basis for Data Collection:
   a. Personal data shall be collected and processed only when there is a lawful basis for doing so, such as consent, contract, legal obligation, vital interests, public task, or legitimate interests.

2. Transparency in Data Collection:
   a. Individuals shall be informed about the purpose and lawful basis for collecting their personal data, and how it will be used, stored, and shared.

DATA USAGE

1. Purpose Limitation:
   a. Personal data shall be used only for the purposes for which it was collected and shall not be further processed in a manner that is incompatible with those purposes.

2. Data Minimization:

a. Only the personal data that is necessary for the specified purposes shall be collected and processed.

DATA STORAGE AND SECURITY

1. Data Security Measures:
   a. Appropriate technical and organizational measures shall be implemented to protect personal data against unauthorized access, loss, destruction, or damage.
2. Access Controls:
   a. Access to personal data shall be restricted to authorized individuals who need the data to perform their job duties.
3. Data Encryption:
   a. Personal data shall be encrypted both in transit and at rest to ensure its security.

DATA SHARING AND DISCLOSURE

1. Third-Party Processors:
   a. Personal data may be shared with third-party processors only when they provide sufficient guarantees to implement appropriate technical and organizational measures to ensure data protection.
2. Legal and Regulatory Requirements:
   a. Personal data may be disclosed to third parties when required by law or regulation.
3. Data Sharing Agreements:
   a. Data sharing with third parties shall be governed by formal agreements that ensure compliance with data protection requirements.

DATA RETENTION AND DESTRUCTION

1. Data Retention Policy:
   a. Personal data shall be retained only for as long as necessary to fulfill the purposes for which it was collected, in accordance with applicable legal and regulatory requirements.
2. Data Destruction:
   a. Personal data that is no longer needed shall be securely destroyed in a manner that ensures it cannot be reconstructed or accessed.

DATA BREACH MANAGEMENT

1. Data Breach Response Plan:
   a. AOU shall have a data breach response plan in place to identify, report, and respond to data breaches in a timely manner.
2. Reporting Data Breaches:
   a. Data breaches shall be reported to the relevant authorities and affected individuals as required by law.

ROLES AND RESPONSIBILITIES

1. Data Protection Officer (DPO):
   a. AOU shall appoint a Data Protection Officer responsible for overseeing data protection strategy and implementation to ensure compliance with data protection laws and policies.

2. Employee Responsibilities:
    a. All employees are responsible for adhering to this policy and attending regular data protection training sessions.

TRAINING AND AWARENESS

1. Data Protection Training:
    a. Regular data protection training shall be provided to all employees to ensure they understand their responsibilities and the importance of data protection.
2. Awareness Campaigns:
    a. AOU shall conduct awareness campaigns to promote best practices in data protection and inform stakeholders about their rights and responsibilities.

REVIEW AND COMPLIANCE

1. Policy Review:
    a. This policy shall be reviewed annually or whenever there are significant changes in data protection laws or practices.
2. Compliance Monitoring:
    a. Regular audits and assessments shall be conducted to ensure compliance with this policy and identify areas for improvement.

CONTACT INFORMATION:

For any questions or concerns regarding this policy or data protection at AOU, please contact:
Data Protection Officer
Email: dpo@aou.edu.ng
Mobile No:.....
AOU Website: www.aou.edu.ng

.....
Prof. Ahmed Salisu Garba
Ag.VC, AOU, Abuja

APPENDIX 1

Storage Limitation

Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed. This principle ensures that personal data is not retained indefinitely and is only kept for as long as it is needed to fulfill its intended purpose. The storage limitation principle involves several key components:

1. Purpose-Driven Retention:
    a. Personal data must be retained only for the period necessary to achieve the purposes for which it was collected. After this period, the data should be securely deleted or anonymized.
    b. Regular reviews and assessments of data retention periods should be conducted to ensure that data is not kept longer than necessary. This includes establishing clear retention schedules and adhering to them.
2. Data Minimization:
    a. Data should not be retained "just in case" it might be useful in the future. Retention should be based on specific, identified purposes.
    b. Only data that is necessary for the specified purpose should be retained. Irrelevant or excessive data should be promptly deleted.
3. Legal and Regulatory Compliance:
    a. Retention periods must comply with relevant legal and regulatory requirements. Certain data may need to be retained for a specific period to comply with laws or regulations.
    b. The retention policies and periods must be documented to ensure compliance and provide transparency.
4. Secure Deletion and Anonymization:
    a. Personal data that is no longer needed should be securely destroyed using methods that ensure it cannot be reconstructed or accessed. This includes physical destruction of paper records and secure deletion of electronic data.
    b. In some cases, data may be anonymized instead of being deleted. Anonymized data cannot be used to identify individuals and may be retained for statistical or research purposes.
5. Exceptions and Special Cases:
    a. In certain circumstances, data may be retained for longer periods if it is being used for archival purposes in the public interest, scientific or historical research, or statistical purposes. In such cases, appropriate safeguards must be in place to protect the data.
    b. Data may be retained for longer periods if it is needed to establish, exercise, or defend legal claims. This must be justified and documented.

Action Plan

1. Establishing Retention Schedules:
    a. AOU will develop and implement clear data retention schedules for different categories of personal data. These schedules will specify the retention periods based on the purpose of data processing, legal requirements, and business needs.
2. Regular Audits and Reviews:

a. Regular audits and reviews of data retention practices will be conducted to ensure compliance with this policy. Any data retained beyond the necessary period will be identified and securely deleted or anonymized.

3. Staff Training and Awareness:
   a. Staff will be trained on the importance of data retention and destruction practices. They will be informed about the procedures for securely deleting or anonymizing data and the need to adhere to retention schedules.
4. Monitoring and Reporting:
   a. The Data Protection Officer (DPO) will monitor compliance with the storage limitation principle and report any issues or non-compliance. Corrective actions will be taken to address any identified problems.

APPENDIX 2

Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. This principle is fundamental to safeguarding the privacy and security of personal data. Here is a detailed breakdown of what this involves:

1. Data Security Measures:
   a. Technical Measures:
      - Personal data should be encrypted both in transit and at rest to prevent unauthorized access. This ensures that even if data is intercepted or accessed without authorization, it cannot be read or used.
      - Implement robust access control mechanisms to ensure that only authorized personnel have access to personal data. This includes the use of strong passwords, multi-factor authentication, and role-based access controls.
      - Use firewalls and antivirus software to protect the university's network and systems from malware, viruses, and other cyber threats.
      - Ensure that all systems and applications used to process personal data are secure and regularly updated with the latest security patches.
   b. Organizational Measures:
      - Establish and enforce comprehensive data protection policies that outline the procedures and responsibilities for ensuring data security.
      - Provide regular training to all employees on data protection and security practices. This includes recognizing phishing attempts, proper handling of personal data, and reporting security incidents.
      - Develop and implement an incident response plan to quickly and effectively respond to data breaches or security incidents. This includes identifying the breach, containing it, assessing the damage, and notifying affected parties and authorities as required.
2. Protection Against Unauthorized Processing:
   a. Access Management:
      - Ensure that individuals have access only to the data necessary for their job functions. This minimizes the risk of unauthorized access and data breaches.

- Monitor user activities on systems and applications that process personal data to detect and respond to suspicious activities promptly.

b. Data Integrity:
   - Implement processes to ensure the accuracy and completeness of personal data. Regularly review and update data to maintain its integrity.
   - Maintain audit trails to track access and modifications to personal data. This helps in identifying and investigating unauthorized activities.

3. Protection Against Accidental Loss, Destruction, or Damage:
   a. Backup and Recovery:
      - Perform regular backups of personal data to ensure that it can be restored in case of accidental loss or data corruption. Store backups in a secure, off-site location.
      - Develop and maintain a disaster recovery plan to ensure the continuity of operations and protection of personal data in case of natural disasters, cyber-attacks, or other emergencies.
   b. Physical Security:
      - Ensure that physical locations where personal data is stored (e.g., server rooms, filing cabinets) are secure and access is restricted to authorized personnel only.
      - Implement environmental controls (e.g., fire suppression systems, climate control) to protect physical data storage locations from damage.
4. Compliance with Legal and Regulatory Requirements:
   a. Data Protection Regulations:
      - Ensure that all data processing activities comply with Nigeria's Data Protection Act of 2023 and relevant international data protection laws and regulations.
      - Conduct DPIAs for new projects or systems that involve significant data processing to identify and mitigate potential privacy risks.
5. Monitoring and Continuous Improvement:
   a. Regular Audits:
      - Conduct regular internal audits to assess the effectiveness of data protection measures and identify areas for improvement.
      - Engage third-party auditors to provide an independent assessment of the university’s data protection practices.
   b. Continuous Improvement:
      - Establish mechanisms for employees and data subjects to provide feedback on data protection practices. Use this feedback to continuously improve data security measures.
      - Keep abreast of the latest developments in data protection and security technologies, practices, and regulations to ensure ongoing compliance and protection.

Action Plan

1. Policy Development:
    a. Develop and implement comprehensive data protection policies that address all aspects of data security, including access controls, encryption, backup procedures, and incident response.
2. Employee Training:
    a. Provide regular training sessions for all employees to ensure they understand their roles and responsibilities in protecting personal data.
3. Technology Investment:
    a. Invest in state-of-the-art security technologies and infrastructure to safeguard personal data.
4. Regular Reviews:
    a. Conduct regular reviews and updates of security measures to address emerging threats and vulnerabilities.

APPENDIX 3

Transparency in Data Collection

Transparency in data collection is a fundamental principle of data protection that ensures individuals are fully informed about how their personal data is being collected, processed, and used. This principle helps build trust between the institution and data subjects, ensuring compliance with legal and regulatory requirements. Here is a detailed elaboration on how AOU implements transparency in data collection:

PURPOSE AND LAWFUL BASIS FOR DATA COLLECTION

1. Clear Communication:
    a. AOU will clearly communicate to individuals the specific purposes for which their personal data is being collected. This includes explaining how the data will be used to support university operations, such as admissions, academic records, research, and alumni relations.
    b. Individuals will be informed about the lawful basis for collecting their personal data. The lawful basis may include consent, contract, legal obligation, vital interests, public task, or legitimate interests. Each basis will be explained in a manner that is easy to understand.
2. Comprehensive Privacy Notices:
    a. Privacy Notices: AOU will provide comprehensive privacy notices at the point of data collection. These notices will detail the purposes of data collection, the types of data collected, the lawful basis for processing, and how the data will be used.
    b. Accessible Information: Privacy notices will be easily accessible on the AOU website and at all points of data collection, such as online forms, registration desks, and mobile applications.

HOW DATA WILL BE USED

1. Specific Use Cases:

a. AOU will provide detailed descriptions of how personal data will be used. This includes academic administration, communication with students and staff, provision of educational services, and compliance with legal obligations.
b. Where applicable, AOU will provide examples and scenarios to illustrate how personal data will be used in practical terms, enhancing understanding and clarity.

2. Data Minimization:
- Relevant and Necessary Data:** AOU will ensure that only data relevant and necessary for the specified purposes is collected. This helps in avoiding the collection of excessive or irrelevant data.

HOW DATA WILL BE STORED

1. Storage Practices:
a. Individuals will be informed about the measures AOU takes to store personal data securely. This includes the use of encryption, access controls, and secure servers.
b. AOU will specify the retention periods for different types of personal data, explaining how long the data will be kept and the criteria for determining retention periods.

2. Access Control:
a. Limited Access: Information about who has access to personal data and the measures in place to ensure that access is restricted to authorized personnel only will be communicated to data subjects.
b. AOU will inform individuals about the use of audit trails to monitor access and changes to personal data, ensuring accountability and security.

HOW DATA WILL BE SHARED

1. Third-Party Sharing:
a. Individuals will be informed if their personal data will be shared with third-party processors or service providers. AOU will provide information about the identity of these third parties and the purposes for which the data will be shared.
b. AOU will disclose that data sharing with third parties is governed by formal agreements that ensure the third parties adhere to data protection standards.

2. Legal and Regulatory Sharing:
a. AOU will inform individuals about situations where their personal data may be shared to comply with legal and regulatory requirements. This includes sharing data with government authorities, regulatory bodies, and law enforcement agencies.
b. In cases where data sharing is based on the individual's consent, AOU will provide clear information on the scope and purpose of the sharing, and the individual's right to withdraw consent at any time.

Action Plan

1. Privacy Notice Development:
a. Develop and regularly update privacy notices to reflect current data processing activities and ensure they are comprehensive and easily understandable.
2. Training and Awareness:
a. Conduct regular training sessions for staff on the importance of transparency in data collection and how to communicate this effectively to individuals.

3. Feedback Mechanisms:
    a. Implement feedback mechanisms, such as surveys and suggestion boxes, to gather input from data subjects on the clarity and comprehensiveness of privacy notices and information provided.
4. Regular Reviews:
    a. Perform regular reviews of data collection practices and privacy notices to ensure they remain up-to-date with legal requirements and best practices.