



FEDERAL UNIVERSITY OF TRANSPORTATION, DAURA

INSTITUTIONAL POLICY

# Institutional Artificial Intelligence Policy

---

This draft sets out how the Federal University of Transportation, Daura expects artificial intelligence to be used responsibly in teaching, learning, research, administration and innovation. It is published for institutional review and does not yet have the force of an approved university policy.

**DRAFT — PENDING INSTITUTIONAL APPROVAL**

**Draft for Institutional Review — Not Yet Approved**

Document reference: FUTD/AI/PL/001 (Provisional)

Version 1.0 (Draft) · Prepared 21 October 2026

Public — Draft for Institutional Review

# Table of Contents

---

|    |                                                    |    |
|----|----------------------------------------------------|----|
| 1  | Policy Information and Document Control            | 4  |
| 2  | Preamble and Institutional Context                 | 5  |
| 3  | Purpose                                            | 5  |
| 4  | Scope and Applicability                            | 6  |
| 5  | Definitions                                        | 6  |
| 6  | Guiding Principles                                 | 8  |
| 7  | Acceptable Uses of AI                              | 9  |
| 8  | AI Use in Teaching and Learning                    | 10 |
| 9  | Academic Integrity and Research Ethics             | 11 |
| 10 | AI in University Administration                    | 12 |
| 11 | Privacy and Data Protection                        | 13 |
| 12 | Information Security                               | 14 |
| 13 | Intellectual Property and Copyright                | 15 |
| 14 | High-Risk and Restricted AI Applications           | 16 |
| 15 | AI Procurement, Integration, and Vendor Management | 17 |

# Table of Contents (continued)

---

|    |                                                        |    |
|----|--------------------------------------------------------|----|
| 16 | Governance and Institutional Responsibilities          | 18 |
| 17 | AI Literacy and Capacity Building                      | 19 |
| 18 | Transparency and Disclosure                            | 19 |
| 19 | Monitoring, Auditing, and Compliance                   | 20 |
| 20 | Complaints, Incidents, and Appeals                     | 20 |
| 21 | Exceptions                                             | 21 |
| 22 | Policy Review and Amendment                            | 21 |
| 23 | Related Laws, Regulations, and References              | 22 |
| 24 | Appendices                                             | 23 |
| A  | Student AI-Use Declaration Template                    | 23 |
| B  | Staff AI-Use Checklist                                 | 24 |
| C  | AI System Risk-Assessment Checklist                    | 24 |
| D  | Guidelines for Using External AI Services              | 25 |
| E  | Examples of Permitted, Restricted, and Prohibited Uses | 26 |
| F  | AI Incident-Reporting Information                      | 26 |

SECTION 1

# Policy Information and Document Control

This section records the identity and control information for the Institutional Artificial Intelligence Policy. Values marked provisional have not been formally assigned by the University and must be confirmed through the appropriate institutional process.

DOCUMENT CONTROL

| Field              | Detail                                                                            |
|--------------------|-----------------------------------------------------------------------------------|
| Institution        | Federal University of Transportation, Daura (FUTD)                                |
| Policy title       | Institutional Artificial Intelligence Policy                                      |
| Policy reference   | FUTD/AI/PL/001 (Provisional — official reference to be assigned)                  |
| Version            | 1.0 (Draft)                                                                       |
| Policy owner       | Directorate of ICT (Proposed — subject to confirmation by the University)         |
| Date prepared      | 21 October 2026                                                                   |
| Approval authority | University Senate, where applicable under the University Statutes and Regulations |
| Approval status    | Draft for Institutional Review — Not Yet Approved                                 |
| Approval date      | Not assigned                                                                      |
| Effective date     | To be assigned following formal approval                                          |
| Review cycle       | Every two years from the effective date, or earlier if required                   |
| Classification     | Public — Draft for Institutional Review                                           |

## Document history

| Version     | Date            | Description                                                                                                             |
|-------------|-----------------|-------------------------------------------------------------------------------------------------------------------------|
| 1.0 (Draft) | 21 October 2026 | Initial draft prepared for institutional review. No approval history exists because the document has not been approved. |

DRAFT STATUS

This document has not been approved by the University Senate. It is published to support institutional review and consultation. Approval, effective dates and any final amendments must be confirmed through the University's established governance process.

## SECTION 2

## Preamble and Institutional Context

---

Artificial intelligence is transforming higher education, research, public administration, engineering and the transportation sector. It is reshaping how knowledge is discovered, how systems are designed and operated, how infrastructure is planned, and how services are delivered. For a university dedicated to transportation, engineering, technology, management and related disciplines, AI presents significant opportunities for innovation, efficiency and national development, as well as serious risks that require deliberate governance.

The Federal University of Transportation, Daura recognises that responsible AI adoption can strengthen teaching and learning, accelerate research, improve administrative services and support advances in intelligent transportation systems, logistics, mobility, infrastructure and sustainable development. The University also recognises that AI can produce inaccurate or fabricated information, reproduce bias, compromise privacy and security, undermine academic integrity, infringe intellectual property and cause harm when used without adequate human oversight.

This policy establishes a human-centred and risk-based framework for the use of AI in the University. It is guided by the University's commitment to academic excellence, integrity, transparency, accountability, inclusion, data protection, information security and responsible innovation. It seeks to enable the University community to benefit from AI while preserving human judgment, protecting the rights of individuals and safeguarding the reputation and resources of the University.

The University's specialisation in transportation and related disciplines gives this policy a particular focus on safety-critical systems, intelligent mobility, logistics optimisation, engineering design, research integrity and the ethical deployment of emerging technologies. The policy is intended to support, rather than replace, existing statutes, regulations, codes of conduct, research ethics requirements and information-security controls.

## SECTION 3

## Purpose

---

The purpose of this policy is to:

1. establish institutional standards for the responsible, lawful and ethical use of artificial intelligence;
2. encourage responsible AI adoption in teaching, learning, research, administration and innovation;
3. protect academic integrity and the integrity of research, assessment and institutional records;
4. safeguard personal data, confidential information, university systems and the rights of individuals;
5. support the effective use of AI to enhance teaching, learning and research outcomes;
6. improve administrative efficiency, service delivery and evidence-based decision-making;
7. promote innovation in transportation, engineering, logistics, mobility and related disciplines;
8. identify, assess, manage and monitor the legal, ethical, operational, security and reputational risks associated with AI; and
9. provide clear accountability, disclosure, review and incident-reporting arrangements.

## SECTION 4

## Scope and Applicability

This policy applies to all persons who use AI for, or in connection with, university activities, including:

- students, including undergraduate, postgraduate, professional and visiting students;
- academic staff, researchers, postdoctoral fellows, teaching assistants and supervisors;
- non-academic staff, administrators, technicians, librarians and support personnel;
- contractors, consultants, vendors, agents and service providers acting for the University;
- visiting scholars, exchange students, affiliates and other authorised users; and
- members of committees, panels and working groups involved in university business.

The policy applies to all faculties, departments, directorates, units, research centres, laboratories, projects and activities of the University. It covers AI systems and tools used on university premises, university-managed devices, university accounts, university networks and university data, as well as AI used elsewhere for official university work.

The policy applies to third-party AI services, including cloud-based generative AI tools, embedded AI features in software, research platforms, learning systems and administrative systems. It also applies to AI components developed, commissioned, integrated or evaluated by the University or on its behalf.

Use of AI for personal purposes that has no connection to university work, university data or the user's role at the University is outside the direct scope of this policy. However, users remain responsible for complying with applicable law, and personal use that affects the University, its members or its reputation may be addressed under the relevant university regulations and codes of conduct.

**EXISTING RULES CONTINUE TO APPLY**

This policy supplements, and does not replace, the University Statutes, academic regulations, examination rules, research ethics requirements, disciplinary procedures, data-protection rules, information-security policies, procurement rules and employment terms.

## SECTION 5

## Definitions

In this policy, the following definitions apply unless the context requires otherwise.

**Artificial intelligence (AI)**

A broad field of computing concerned with systems that perform tasks associated with human intelligence, including learning, reasoning, prediction, language processing, perception, planning and decision support.

**Generative AI**

AI systems that generate new text, images, audio, video, code or other outputs in response to prompts, usually by learning patterns from large datasets.

---

**Large language model (LLM)**

A type of generative AI model trained on large volumes of text to predict and produce language, and which may also process code, images or other data depending on the system.

---

**AI-assisted work**

Any work, output, decision, analysis or communication in which AI has been used to generate, transform, analyse, summarise, draft, translate, recommend or otherwise support human activity.

---

**Automated decision-making**

The use of an AI system to make or substantially determine a decision with little or no meaningful human involvement.

---

**High-impact AI use**

A use of AI that may significantly affect a person's rights, opportunities, safety, finances, employment, education, reputation or access to university services, or that supports a safety-critical transportation system.

---

**Personal data**

Information relating to an identified or identifiable living individual, as defined under the Nigeria Data Protection Act 2023 and applicable subsidiary guidance.

---

**Sensitive personal data**

Personal data falling within the special categories recognised by applicable data-protection law, including health data, biometric data, genetic data, data relating to children, and other information requiring enhanced protection.

---

**Confidential information**

Information that is not publicly available and that the University is obliged or entitled to protect, including unpublished research, examination materials, personnel records, financial records, security information, commercial information and information received under a duty of confidence.

---

**Human oversight**

Meaningful human review, judgment and accountability over the use and outputs of an AI system, including the authority to question, correct, suspend or reject an AI output or decision.

---

**AI-generated content**

Text, code, images, audio, video, data, recommendations or other material produced by an AI system, whether or not subsequently edited by a human.

---

**AI hallucination**

A plausible but false or unsupported output produced by an AI system, including fabricated facts, references, quotations, calculations, events or code behaviour.

---

**Responsible AI**

The development, procurement and use of AI in a manner that respects human rights, safety, privacy, fairness, transparency, accountability, academic integrity and the public interest.

---

**AI system owner**

The person, unit or committee with delegated responsibility for the approval, operation, oversight and review of a particular AI system or use case.

---

## Prompt

The instruction, question, text, code, file or other input provided to an AI system to elicit an output.

## SECTION 6

# Guiding Principles

The use of AI at the University shall be guided by the following principles.

### Human oversight and accountability

AI shall support, not displace, human judgment and institutional accountability. A named person or unit must remain responsible for any AI-assisted decision, output or system.

### Transparency and disclosure

AI use shall be disclosed where it materially affects academic work, research, official decisions, publications, reports or communications, in accordance with this policy and the relevant academic or professional rules.

### Fairness and non-discrimination

AI shall not be used to unlawfully discriminate against individuals or groups. Users and system owners shall take reasonable steps to identify, assess and mitigate bias.

### Privacy and data protection

AI shall be used in a manner consistent with the Nigeria Data Protection Act 2023, applicable guidance and the University's data-protection requirements. Personal data shall be processed lawfully, fairly and transparently.

### Security and safety

AI systems and outputs shall be assessed for security, reliability and safety risks, particularly where they affect critical infrastructure, transportation operations or the safety of persons.

### Accuracy and verification

AI outputs shall be treated as unverified by default. Users shall verify facts, calculations, citations, code and recommendations against reliable sources before relying on them.

### Academic integrity

AI use shall not undermine the authenticity of assessment, the integrity of research or the recognition of human contribution.

### Accessibility and inclusion

AI adoption shall take account of accessibility, equity and inclusion, and shall not create unjustified barriers for persons with disabilities or other underrepresented groups.

### Intellectual property protection

AI use shall respect copyright, database rights, software licences, contractual obligations and the University's intellectual-property interests.

### Proportionality and risk management

The controls applied to an AI use shall be proportionate to the likelihood and severity of potential harm, the sensitivity of the data involved and the significance of the decision or activity affected.

---

**Environmental and resource awareness**

The University shall consider the energy, computational and environmental costs of AI systems and shall encourage efficient, appropriate and sustainable use.

---

**SECTION 7****Acceptable Uses of AI**

---

Subject to this policy, the relevant academic, research, administrative and information-security requirements, AI may be used to support the following activities.

**Teaching and lesson preparation**

Drafting lesson plans, generating examples, developing practice questions, creating accessible learning materials and exploring alternative explanations, subject to lecturer review and quality assurance.

**Student learning and revision**

Explaining concepts, generating practice problems, summarising approved materials, testing understanding, practising languages and supporting study planning, provided that submitted work complies with assessment rules.

**Programming and software development**

Generating code suggestions, debugging, explaining errors, drafting tests and documenting software, subject to human review, testing and compliance with security and licensing requirements.

**Research assistance**

Brainstorming research questions, structuring literature searches, summarising public sources, drafting plans and assisting with analysis, subject to researcher verification and research-ethics obligations.

**Data analysis and visualisation**

Assisting with data cleaning, exploratory analysis, statistical code, visualisation and interpretation, using approved datasets and with validation of outputs.

**Literature discovery and summarisation**

Identifying potentially relevant sources, summarising publicly available material and generating search terms, provided that citations and claims are independently verified.

**Transportation research and simulation**

Supporting modelling, simulation, optimisation, scenario analysis and engineering design in transportation and related fields, with appropriate validation and human oversight.

**Intelligent transport systems**

Supporting research, planning and operational analysis for intelligent mobility, traffic management, rail systems, aviation, maritime operations and logistics, subject to safety and security review.

**Logistics optimisation**

Assisting with route planning, inventory analysis, scheduling, demand forecasting and supply-chain modelling, with human review of assumptions and outputs.

**Administrative correspondence**

Drafting routine emails, notices, minutes, reports and service responses, subject to review by the responsible officer

and compliance with records-management requirements.

---

### Document drafting and editing

Improving clarity, structure, grammar, formatting and accessibility of documents, while preserving accuracy and confidentiality.

---

### Accessibility support

Generating captions, transcripts, alternative text, plain-language summaries and other accessibility aids, with human review for accuracy and context.

---

### Library and information services

Supporting catalogue enrichment, search assistance, research guides and information literacy, subject to professional review and licensing constraints.

---

### Innovation and entrepreneurship

Exploring ideas, developing prototypes, testing business models and supporting technology transfer, subject to intellectual-property, procurement and research-ethics requirements.

---

#### PERMISSION IS CONTEXT-DEPENDENT

The examples above are not blanket authorisations. Permission to use AI depends on the relevant academic rules, assessment instructions, research-ethics approvals, confidentiality obligations, contractual terms, information-security requirements and the risk level of the activity.

## SECTION 8

# AI Use in Teaching and Learning

---

The University encourages the thoughtful use of AI to enhance teaching and learning. At the same time, assessment and academic awards must remain credible evidence of the learner's knowledge, skills and authorship. Academic staff and students share responsibility for ensuring that AI use supports, rather than undermines, learning.

### Responsibilities of academic staff

- state clearly in the course outline, assessment brief or examination instructions whether AI use is permitted, restricted or prohibited for each assessment task;
- explain the purpose and limits of permitted AI use, including any requirement to disclose or acknowledge it;
- design assessment and learning activities that test genuine understanding, reasoning, application and disciplinary skills;
- review AI-generated teaching materials for accuracy, bias, accessibility and appropriateness before use;
- avoid uploading examination materials, unpublished research, student records or other restricted information to unapproved AI services;

- provide reasonable guidance on verification, referencing and responsible use; and
- apply the University's academic-integrity procedures fairly and consistently where concerns arise.

## Responsibilities of students

- use AI only where permitted by the course or assessment instructions;
- disclose substantial AI assistance in the manner required by the lecturer or programme;
- verify facts, quotations, references, calculations and code produced with AI assistance;
- retain sufficient records of their own work and contribution where required;
- ensure that submitted work reflects their own understanding and does not misrepresent AI-generated work as independently produced;
- comply with examination and assessment restrictions, including restrictions on devices, software, communication and unauthorised assistance; and
- seek clarification from the lecturer or programme before using AI where the rules are unclear.

## Assessment and academic judgment

Lecturers and examiners may set assessment tasks that require, permit, restrict or prohibit AI use. They may require an AI-use declaration, an oral assessment, an in-class task, a reflective account of the student's process, or other evidence of learning. Any such requirement must be communicated clearly and applied consistently.

The use of AI does not, by itself, constitute academic misconduct. A concern about AI-assisted work must be assessed through a fair review of the available evidence and the applicable academic-integrity procedures. AI-generated work must not automatically be treated as proof of misconduct.

### EXAMINATIONS

The use of AI during an examination or other controlled assessment is permitted only where the examination instructions expressly allow it. Unauthorised use may be dealt with under the University's examination and academic-integrity regulations.

## SECTION 9

# Academic Integrity and Research Ethics

Academic integrity and research ethics are fundamental to the University's mission. AI may assist scholarship, but it must not be used to misrepresent authorship, fabricate evidence, distort findings or conceal the contribution of others.

## Prohibited conduct

- presenting AI-generated text, code, images, data or other content as independently produced where the applicable rules require disclosure;
- fabricating or falsifying references, quotations, data, results, observations or research findings;

- presenting AI-generated data as genuine experimental observations or as data collected from human participants without the required authorisation and validation;
- using AI to impersonate another person or misrepresent the source of work;
- using AI to circumvent examination, assessment or research-ethics controls; and
- using AI in a manner that infringes copyright, confidentiality, privacy or contractual obligations.

## Research expectations

- researchers must understand and comply with the requirements of ethics committees, funders, publishers, collaborating institutions and data providers;
- AI assistance should be acknowledged in dissertations, theses, publications, grant proposals and reports where it materially contributed to the work, in accordance with the applicable rules;
- authors must be able to explain and defend the methods, analysis and conclusions of their work, including any AI-assisted components;
- AI must not be used to generate or analyse data from human participants without appropriate ethics approval, consent, data-protection safeguards and validation;
- unpublished research, confidential peer-review materials, participant data and commercially sensitive information must not be submitted to unapproved AI services; and
- supervisors and research leaders must provide appropriate guidance and oversight to students and early-career researchers.

### AUTHORSHIP

AI systems should not be listed as authors. Human authors remain responsible for the accuracy, integrity and originality of the work, and for acknowledging material AI assistance in accordance with the applicable publication and institutional requirements.

Concerns about academic integrity or research misconduct will be handled under the University's existing academic-integrity, research-ethics and disciplinary procedures. This policy does not create new penalties.

## SECTION 10

# AI in University Administration

AI may be used to improve the efficiency, consistency and quality of administrative services, provided that its use is lawful, transparent, secure and subject to appropriate human oversight.

Administrative areas in which AI may be considered include:

- admissions processing and applicant support;
- student records, registration and academic advising;
- bursary, fees and financial administration;
- human resources, recruitment and staff administration;

- procurement, contract management and supplier assessment;
- customer support, enquiries and service delivery;
- institutional reporting, analytics and planning;
- communications, publications and public information;
- ICT operations, service management and security monitoring; and
- library, records and information management.

#### **NO AUTONOMOUS FINAL DECISIONS**

AI must not independently make final decisions affecting admissions, grades, graduation, disciplinary outcomes, employment, financial entitlements, access to services or other significant rights. Any use of AI in a consequential decision must be authorised, documented, lawful and subject to meaningful human review.

### **Human review requirements**

- the responsible officer must have the authority, information and practical ability to review the AI output;
- the basis of a consequential decision must be explainable and, where appropriate, communicated to the affected person;
- affected persons must have access to the University's existing complaint, review or appeal procedures;
- AI must not be used to bypass established eligibility, financial-control, procurement or records-management rules; and
- decisions and supporting evidence must be retained in accordance with the University's records-management and data-protection requirements.

#### **SECTION 11**

## **Privacy and Data Protection**

The University processes personal data in accordance with the Nigeria Data Protection Act 2023, applicable subsidiary regulations and guidance, and the University's data-protection requirements. AI use must not weaken those protections.

The following categories of information require particular care:

- student records, applications, assessment results and disciplinary records;
- staff records, recruitment information, payroll data and performance records;
- examination questions, marking schemes, moderation records and results before publication;
- financial records, bank details, payment information and procurement data;
- medical, disability, counselling and other sensitive personal data;
- research participants' data, consent records and identifiable research materials;

- credentials, passwords, authentication tokens, API keys and security configurations;
- confidential institutional documents, legal advice, internal audit findings and security reports; and
- personal information processed by external AI providers on behalf of the University.

## Data-protection obligations

- process personal data only for lawful, specified and legitimate purposes;
- collect and submit only the data that is necessary for the task;
- use approved AI services and approved configurations for university data;
- apply appropriate access controls, encryption and retention rules;
- avoid entering identifiable or sensitive data into AI tools unless the use is authorised and appropriate safeguards are in place;
- assess third-party AI providers for data-protection, security, retention, deletion and sub-processing risks before use;
- respect data-subject rights and the University's procedures for handling requests; and
- report suspected data breaches promptly through the University's existing incident procedures.

### RESTRICTED INFORMATION

Users must not submit restricted university information, sensitive personal data, examination materials, confidential research or credentials to unapproved AI services. Where a tool is not approved for the relevant data classification, the data must not be entered.

## SECTION 12

# Information Security

AI systems introduce information-security risks that must be managed in accordance with the University's information-security requirements and applicable law, including the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended.

Users and system owners shall consider the following risks:

- prompt injection, hidden instructions and malicious content designed to manipulate AI outputs or connected systems;
- insecure or untested AI-generated source code, scripts, configurations or infrastructure commands;
- disclosure of secrets, credentials, tokens, personal data or confidential information through prompts or logs;
- phishing, impersonation, deepfakes and fraudulent communications generated or assisted by AI;
- malware, malicious extensions, unapproved plugins and compromised third-party services;
- unauthorised integrations between AI tools and university systems;
- data leakage, unauthorised retention and unclear deletion practices by external providers; and

- over-reliance on AI recommendations without human verification.

## Security controls

- AI-generated code must be reviewed, tested and approved before use in production or on university systems;
- commands, scripts and configuration changes generated by AI must be verified by a competent person before execution;
- secrets and credentials must not be entered into AI tools and must be managed through approved secret-management arrangements;
- AI services must be procured and integrated through the established ICT, procurement and security review processes;
- access to AI systems must follow least-privilege and authentication requirements; and
- suspected security incidents must be reported immediately through the University's existing incident-reporting channels.

### VERIFY BEFORE YOU EXECUTE

AI-generated commands, code, links and recommendations may be incorrect or malicious. A human with appropriate competence must verify and authorise them before they are executed, deployed or relied upon.

## SECTION 13

# Intellectual Property and Copyright

AI use must respect intellectual property rights and contractual obligations. This includes the Copyright Act 2022, software licences, database rights, confidentiality obligations, research agreements and the University's intellectual-property requirements.

- human-created work remains subject to the applicable ownership, authorship and licensing rules;
- third-party copyrighted material must not be reproduced, adapted or distributed without lawful authority;
- AI tools must not be used to circumvent paywalls, licence restrictions, access controls or contractual terms;
- AI-generated content must be reviewed for potential infringement before publication or commercial use;
- software and code generated with AI assistance must be checked for licence compatibility and security;
- research outputs must comply with funder, publisher and collaborator requirements;
- university-owned intellectual property and confidential commercial information must be protected; and
- attribution and disclosure must be provided where required by law, contract or academic convention.

**NO BLANKET OWNERSHIP CLAIM**

The copyright status of AI-generated outputs is unsettled and may depend on human authorship, the terms of the AI service, the source material used and applicable law. This policy does not assert blanket ownership or copyright over AI-generated content. Each case must be assessed on its facts and the relevant legal and contractual requirements.

**SECTION 14****High-Risk and Restricted AI Applications**

Additional review is required before AI is used in high-risk or restricted applications. The level of review must be proportionate to the potential impact on individuals, safety, institutional operations and the University's reputation.

High-risk applications include:

- high-impact student assessment, progression, admission or graduation decisions;
- recruitment, promotion, discipline or employment decisions;
- decisions affecting financial entitlements, scholarships, fees or payments;
- identity verification and access control;
- biometric identification, emotion recognition, surveillance and monitoring;
- disciplinary investigations, misconduct reviews and safeguarding matters;
- processing of sensitive personal data or data relating to vulnerable persons;
- safety-critical transportation systems, infrastructure and operations;
- autonomous or intelligent transportation research with real-world safety implications; and
- any decision or system with substantial consequences for individuals or the public.

**Additional requirements**

- a documented risk assessment addressing lawfulness, fairness, safety, security, privacy, bias, accuracy and human rights;
- appropriate authorisation from the responsible university authority and, where required, the relevant committee;
- testing and validation using representative data and realistic conditions;
- meaningful human oversight with the authority to override, suspend or stop the system;
- transparency to affected persons and access to review or appeal procedures;
- monitoring, logging, incident reporting and periodic revalidation; and
- an exit, suspension or fallback plan if the system fails or causes harm.

**SAFETY-CRITICAL SYSTEMS**

AI must not be deployed in safety-critical transportation systems or operations unless the relevant engineering, operational, security and regulatory requirements have been met and human oversight is maintained.

**SECTION 15****AI Procurement, Integration, and Vendor Management**

The acquisition or institutional deployment of AI services must follow the University's procurement, ICT, legal, data-protection and information-security requirements. AI must not be adopted through informal or unauthorised arrangements.

Before acquiring or integrating an AI service, the responsible unit shall assess:

- the lawful basis, purpose and necessity of the processing;
- data-protection and privacy risks, including retention, deletion and sub-processing;
- information-security controls, incident history and breach-notification arrangements;
- licensing, intellectual-property and usage restrictions;
- accessibility and inclusion requirements;
- reliability, accuracy, performance and testing arrangements;
- total cost, including implementation, training, support and exit costs;
- vendor terms, service levels, liability, audit rights and termination rights;
- data location, sovereignty and transfer arrangements;
- integration requirements and compatibility with university systems;
- institutional ownership of data, configurations and outputs; and
- exit arrangements, data extraction and deletion on termination.

Contracts and vendor arrangements should include appropriate data-protection, confidentiality, security, audit, notification, retention, deletion, service-level and termination provisions. Vendors must not use university data for unrelated purposes, including model training, unless expressly authorised under a lawful and documented arrangement.

**PROPOSED RESPONSIBILITIES**

The Directorate of ICT should coordinate technical and security assessment; the Bursary and Procurement Unit should apply the University's procurement rules; the Registry and Legal Unit should review contractual and governance issues; and the relevant data-protection arrangements should be applied. These arrangements are subject to confirmation of the University's actual governance structure.

**SECTION 16**

## Governance and Institutional Responsibilities

---

Effective AI governance requires clear responsibilities across the University. This section distinguishes existing university authorities from arrangements that are proposed and subject to confirmation.

### University Senate

The University Senate, where applicable under the University Statutes and Regulations, is the proposed approval authority for this policy and for significant amendments. No claim is made that the Senate has approved this draft.

### Vice-Chancellor

The Vice-Chancellor provides institutional leadership for AI governance and may designate responsibility for implementation, oversight and escalation.

### Directorate of ICT

The Directorate of ICT is proposed to coordinate the technical implementation of this policy, maintain approved AI service arrangements, support risk assessment and incident response, and provide advice on information security.

### Faculties and academic departments

Faculties and departments are responsible for applying the policy in teaching, assessment and discipline-specific research, and for defining permitted AI use in their programmes.

### Research and postgraduate administration

Research and postgraduate offices are responsible for integrating AI requirements into research ethics, supervision, thesis examination and grant administration.

### Registry

The Registry is responsible for applying the policy to student records, admissions, examinations, academic governance and related administrative processes.

### Bursary

The Bursary is responsible for applying the policy to financial administration, payments, entitlements and related controls.

### Human Resources

Human Resources is responsible for applying the policy to recruitment, employment, performance and staff-development processes.

### Library services

The Library is responsible for applying the policy to information services, research support, licensing and AI literacy.

### Students

Students are responsible for using AI lawfully and ethically, complying with assessment rules, disclosing material assistance where required and verifying AI-generated content.

### Academic and non-academic staff

Staff are responsible for using AI in accordance with this policy, their professional obligations, data-protection rules, information-security requirements and their delegated authority.

---

## Designated AI governance arrangements

The University may establish an AI governance committee, working group or designated officer. Until such arrangements are formally established, the Directorate of ICT should coordinate the policy's implementation in consultation with the relevant offices.

### PROPOSED, NOT EXISTING

References to proposed committees, coordination arrangements or designated responsibilities in this draft do not confirm that such bodies or offices currently exist. They must be reviewed and confirmed by the University before approval.

## SECTION 17

# AI Literacy and Capacity Building

The University is committed to building the AI literacy and professional capability needed to use AI responsibly. Training should be proportionate to role, risk and discipline.

Capacity-building should cover:

- the capabilities and limitations of AI systems, including hallucinations and uncertainty;
- prompt literacy and the importance of clear, lawful and privacy-conscious instructions;
- verification of facts, citations, calculations, code and recommendations;
- academic integrity, assessment design and disclosure requirements;
- research ethics, authorship, data management and publication requirements;
- data protection, confidentiality and permissible data classifications;
- cybersecurity, prompt injection, phishing and safe use of AI tools;
- bias, fairness, accessibility and inclusive design;
- discipline-specific applications in transportation, engineering, logistics, management and related fields; and
- procurement, risk assessment and oversight responsibilities for managers and system owners.

The University should provide induction for new staff and students, targeted training for high-risk roles and periodic refresher opportunities. Faculties, departments and directorates should identify their specific training needs and share good practice.

## SECTION 18

# Transparency and Disclosure

Transparency supports trust, accountability and academic integrity. Users should disclose material AI assistance in a clear, proportionate and honest manner.

Disclosure is particularly important where AI:

- materially contributes to submitted academic work or assessment;
- supports research design, analysis, interpretation or writing in a way that affects authorship or findings;
- generates content in official reports, publications or public communications;
- informs a consequential administrative decision; or
- is used in a high-risk or restricted application.

Trivial uses, such as ordinary spelling correction, grammar checking or routine formatting, do not require disclosure unless a specific assessment or institutional rule requires it. A disclosure should identify the tool where appropriate, describe how it was used and state what human review or verification was undertaken.

#### SAMPLE AI-USE DECLARATION

I used [tool or service] on [date] to assist with [purpose, for example drafting, summarising, coding, data analysis or editing]. I reviewed and verified the output, corrected errors where necessary, and confirm that the final work reflects my own understanding and contribution. Any limitations or unverified content are identified below: [details]. Signed: [name], [student/staff number], [date].

#### SECTION 19

## Monitoring, Auditing, and Compliance

The University will monitor the implementation of this policy on a risk-based basis. Monitoring and auditing must respect privacy, confidentiality, academic freedom and applicable law.

- maintain an inventory of approved AI systems and significant use cases;
- review high-risk uses before deployment and at appropriate intervals;
- monitor incidents, complaints and emerging risks;
- review contracts, vendor arrangements and data-protection terms periodically;
- conduct authorised audits of AI systems and related records where necessary;
- document risk assessments, approvals, testing, training and review outcomes;
- report significant issues to the appropriate university authority; and
- use monitoring data to improve guidance, training and controls.

Monitoring must not involve unnecessary surveillance of individuals. Any monitoring of communications, systems or activities must be lawful, proportionate, transparent where appropriate and consistent with the University's policies and legal obligations.

#### SECTION 20

## Complaints, Incidents, and Appeals

The University will take concerns about AI seriously and will respond through its existing procedures. Reports may concern:

- inaccurate, misleading or harmful AI-generated content;
- discrimination, bias or unfair treatment;
- privacy or data-protection breaches;
- security incidents, misuse or unauthorised access;
- academic-integrity concerns;
- errors in an AI-assisted administrative decision; or
- retaliation against a person who raises a concern in good faith.

Academic-integrity matters should be referred under the University's academic-integrity and examination procedures. Student complaints and appeals should follow the existing student complaint and appeal routes. Staff matters should follow the applicable human-resources and grievance procedures. Data-protection and security incidents should be reported through the University's existing data-breach and cybersecurity incident processes.

#### NO NEW APPEAL BODIES

This policy does not create new disciplinary, grievance or appeal bodies. It directs complaints and appeals to the relevant existing university procedures and responsible offices.

## SECTION 21

# Exceptions

Exceptions to this policy may be authorised only through a controlled process. An exception must be justified, time-limited, documented and reviewed.

1. submit a written request describing the proposed use, purpose and duration;
2. identify the specific policy requirement that cannot be met and explain why;
3. complete a risk assessment covering lawfulness, privacy, security, safety, fairness and academic integrity;
4. identify the safeguards, human oversight and monitoring that will apply;
5. obtain approval from the responsible university authority, in consultation with the Directorate of ICT and any other relevant office;
6. record the decision, conditions and expiry date; and
7. review the exception before expiry and either renew, amend or terminate it.

An exception must not be used to authorise unlawful processing, a prohibited use, an unapproved high-risk deployment or a breach of a contractual or professional obligation. Exceptions must be reported in the periodic review of this policy.

## SECTION 22

# Policy Review and Amendment

This policy should be reviewed every two years from its effective date, or earlier if required. The review should

consider technological developments, institutional experience, incidents, audit findings, changes in applicable law and guidance from relevant authorities.

An earlier review may be triggered by:

- a significant change in AI technology or its use at the University;
- a serious incident, complaint or audit finding;
- a change in Nigerian law, regulation or regulatory guidance;
- a change in university statutes, academic regulations or governance arrangements;
- a significant procurement or integration of a new AI system; or
- a request from the University Senate, the Vice-Chancellor or another authorised body.

Amendments must be approved through the appropriate university governance process. Version control, document history and communication of changes should be maintained.

### SECTION 23

## Related Laws, Regulations, and References

The following materials are relevant to this policy. Their application should be verified against the current official text and any subsequent amendment or guidance.

- Nigeria Data Protection Act 2023, together with applicable regulations, guidance and decisions of the Nigeria Data Protection Commission;
- Copyright Act 2022 (Act No. 8 of 2022) and related copyright regulations;
- Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, and related cybersecurity requirements;
- applicable Nigerian laws and regulations relating to human rights, equality, labour, consumer protection, records, electronic transactions and public procurement;
- the University Statutes, academic regulations, examination regulations, research-ethics requirements and disciplinary procedures;
- University information-security, data-protection, records-management and procurement policies;
- UNESCO Recommendation on the Ethics of Artificial Intelligence (2021);
- UNESCO Guidance for Generative AI in Education and Research (2023); and
- national AI policy and guidance applicable to Nigeria, including the National Artificial Intelligence Strategy (2024), where relevant.

#### LEGAL REVIEW

This draft is not legal advice. The University's Legal Unit and relevant regulatory offices should review the final policy and its references before approval to confirm that all legal and regulatory requirements are accurately reflected.

## SECTION 24

## Appendices

The appendices provide practical tools for implementing this policy. They are intended to be adapted to the specific requirements of faculties, departments and administrative units, subject to approval.

- Appendix A: Student AI-use declaration template;
- Appendix B: Staff AI-use checklist;
- Appendix C: AI system risk-assessment checklist;
- Appendix D: Guidelines for using external AI services;
- Appendix E: Examples of permitted, restricted and prohibited uses; and
- Appendix F: AI incident-reporting information.

## APPENDIX A

## Student AI-Use Declaration Template

Students should use this template where a course or assessment requires a declaration of AI assistance. It should be completed honestly and adapted to the instructions provided by the lecturer.

### *Student AI-Use Declaration*

*Student name: [Full name]*

*Student number: [Student number]*

*Programme: [Programme]*

*Course code and title: [Course code and title]*

*Assessment title: [Assessment title]*

*Date: [Date]*

*AI tool or service used: [Name of tool or service]*

*Purpose of use: [For example brainstorming, drafting, summarising, coding, data analysis, editing or translation]*

*Extent of use: [Describe the parts of the work affected]*

*Prompts or instructions used: [Summarise or attach where required]*

*Output incorporated: [Describe what was used, adapted or rejected]*

*Verification undertaken: [Describe how facts, references, calculations, code or other content were checked]*

*Human contribution: [Explain your own contribution and understanding]*

*Limitations or unverified content: [Identify any]*

*Declaration: I confirm that this declaration is accurate, that I have complied with the assessment instructions, and that I remain responsible for the final work.*

*Signature: [Signature or typed name]*

*Date: [Date]*

ASSESSMENT RULES PREVAIL

This template does not authorise AI use. Students must follow the specific instructions for the course or assessment.

APPENDIX B

Staff AI-Use Checklist

Before using AI for university work, staff should consider the following checklist.

- Is the use consistent with my role, delegated authority and professional obligations?
- Is the AI tool approved for the data classification involved?
- Have I removed or minimised personal, confidential or sensitive information?
- Am I permitted to submit this information to the service under its terms and the University's contracts?
- Have I checked the output for accuracy, bias, safety, accessibility and legal risk?
- Have I verified citations, calculations, code and factual claims?
- Is human review and accountability clearly assigned?
- Does the use require disclosure, consultation, risk assessment or formal approval?
- Have I retained appropriate records and avoided unauthorised data retention?
- Do I know how to report an error, security incident or data breach?

APPENDIX C

AI System Risk-Assessment Checklist

The following checklist supports the assessment of an AI system or use case. It should be completed by the system owner in consultation with the Directorate of ICT, data-protection, legal and other relevant officers.

AI SYSTEM RISK-ASSESSMENT CHECKLIST

| Area                  | Questions to consider                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Purpose and necessity | What problem does the system address? Is AI necessary and proportionate? What are the alternatives?                                     |
| Lawfulness            | What is the lawful basis? Are there legal restrictions on the data or decision? Has legal review been obtained where required?          |
| Data protection       | What personal data is processed? Is it minimised? Where is it stored? What are the retention, deletion and sub-processing arrangements? |
| Security              | What are the authentication, access, encryption, logging and incident-response arrangements? Has the vendor been assessed?              |
| Fairness and bias     | Could the system produce discriminatory or unjustified outcomes? How will bias be tested and monitored?                                 |

| Area                        | Questions to consider                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Accuracy and reliability    | How accurate is the system? What testing, validation and performance monitoring will be used?                                    |
| Safety                      | Could the system affect the safety of persons or critical transport operations? What safeguards and fallback arrangements apply? |
| Human oversight             | Who is accountable? Can a human review, override or stop the system? Is the oversight meaningful?                                |
| Transparency                | Are affected persons informed? Is the basis of significant decisions explainable? Is disclosure required?                        |
| Rights and redress          | How can affected persons complain, request review or appeal? Are existing procedures adequate?                                   |
| Intellectual property       | Are the inputs, outputs, software and data used lawfully? Are licences and contractual terms respected?                          |
| Accessibility and inclusion | Is the system accessible? Could it create barriers for persons with disabilities or other groups?                                |
| Vendor and exit             | What are the service levels, audit rights, termination rights and exit arrangements? Can data be extracted and deleted?          |
| Monitoring and review       | How will the system be monitored, audited and reviewed? What triggers suspension or termination?                                 |

## APPENDIX D

## Guidelines for Using External AI Services

External AI services, including public chatbots and cloud platforms, may process inputs on systems outside the University's direct control. Users should follow these guidelines.

- use only services approved for the relevant data classification and purpose;
- do not enter personal data, sensitive personal data, examination materials, unpublished research or confidential institutional information unless the use is expressly authorised;
- do not enter passwords, API keys, authentication tokens or other secrets;
- review the service's terms, privacy notice, data-retention practices and model-training policies;
- disable or avoid features that retain, publish or share inputs where the service permits;
- use institutional accounts and approved configurations where available;
- verify outputs before relying on them and retain evidence of human review;
- do not connect external AI services to university systems without approval; and
- report suspected data leakage, security incidents or unexpected behaviour promptly.

APPENDIX E

Examples of Permitted, Restricted, and Prohibited Uses

The following examples are illustrative. The specific rules for a course, research project, administrative process or system may be more restrictive. When in doubt, seek guidance before proceeding.

ILLUSTRATIVE EXAMPLES

| Category                              | Examples                                                                                                                                                                                                                                                                                      | Conditions                                                                                                             |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Generally permitted                   | Brainstorming ideas; explaining concepts; drafting routine correspondence; improving grammar; generating practice questions; summarising publicly available material; assisting with code while testing and reviewing it.                                                                     | Comply with assessment, research, confidentiality, security and licensing rules; verify outputs.                       |
| Permitted with conditions or approval | Using AI with internal documents; analysing research data; assisting with student feedback; supporting administrative decisions; integrating an AI tool with a university system; using AI in a high-impact process.                                                                          | Use approved tools and data; complete risk assessment; obtain required approval; maintain human oversight and records. |
| Restricted                            | High-impact assessment; recruitment and employment decisions; financial entitlements; identity verification; biometrics and surveillance; disciplinary investigations; safety-critical transport systems; processing sensitive personal data.                                                 | Additional authorisation, documented risk assessment, testing, transparency, human review and monitoring are required. |
| Prohibited                            | Submitting restricted data to unapproved AI services; fabricating research data or references; impersonation; bypassing security controls; generating or distributing unlawful or harmful content; allowing AI to make final decisions on significant rights without an authorised framework. | Must not be undertaken. Report suspected misuse through the appropriate university procedure.                          |

APPENDIX F

AI Incident-Reporting Information

An AI incident includes any actual or suspected event involving AI that causes or may cause harm, data loss, unauthorized access, discrimination, safety risk, academic-integrity concern, reputational damage or significant

operational disruption.

1. stop using the system or process where there is an immediate risk to safety, security, data or individuals;
2. preserve relevant records, screenshots, logs and evidence without altering them;
3. report the incident promptly to the Directorate of ICT and the responsible unit;
4. where personal data may be affected, follow the University's existing data-breach reporting procedure;
5. where a student or staff matter is involved, follow the relevant academic-integrity, disciplinary, grievance or safeguarding procedure;
6. cooperate with containment, investigation and remediation; and
7. record the incident, actions taken and lessons learned for periodic review.

#### CONTACT

Policy and incident enquiries may be directed to the Directorate of ICT through [info@futd.edu.ng](mailto:info@futd.edu.ng) or the Directorate's existing contact arrangements. This draft does not create a new incident hotline or reporting body.